مقدمة في الشبكات
Introduction To Network

what's Network? ما هي الشبكة

Network is a group of Computers Connected with other to share Data.

هي مجموعة من الحواسيب متصلة مع بعض لمشاركة البيانات

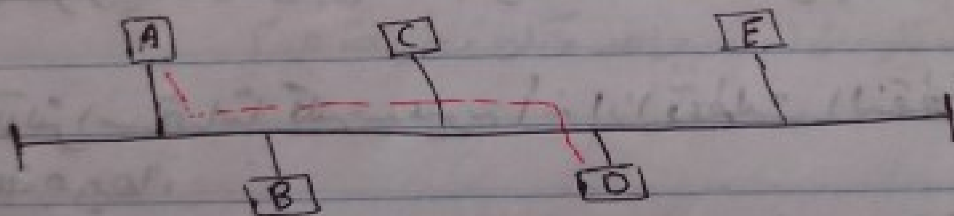
Network Components مكونات الشبكة

1- PC's اجهزة الكمبيوتر
2- Cables الكابلات
3- Network devices: Router - Switch - NIC, Hub ... Modem & Repeater

الموجه المحول كارت الشبكة

Network Topologies بنية أو طبيعة الشبكات

① Bus Topology ① الشبكة الخطية

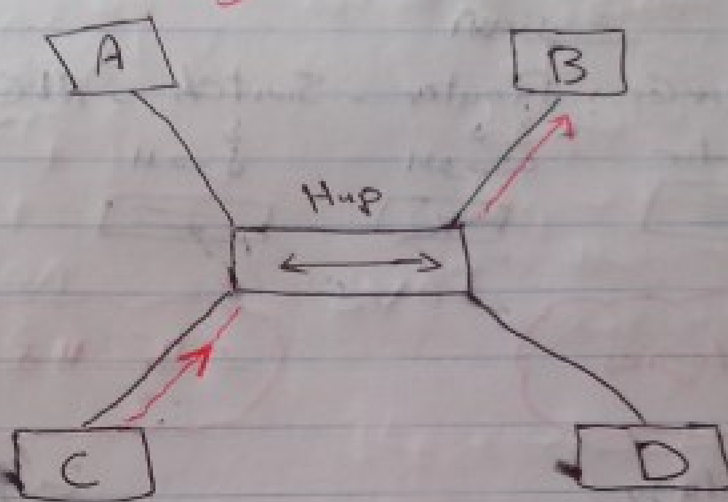


في هذه الطريقة إذا كان A يرسل إلى D البيانات تصل إلى جميع الاجهزة E و B و C وايضا يعيب وهو half duplex

وهو أنه تكون هناك قناة واحدة للارسال والاستقبال ومثال على ذلك أجهزة اللاسلكي في استخدام رجال الشرطة لها فالطرف الاول يتكلم ثم يقول [حول] حتى يعلم الطرف الثاني أنه انتهى من الكلام فيستطيع الطرف الثاني

أن يتكلم و الطرف الاول أن يستمع له وهكذا.
ومن عيوب هذا النوع أيضا أنه إذا كان A يرسل إلى B فلا يستطيع
C أن يرسل إلى D إلا بعد انتهاء عملية النقل بين A ، B
- أمثلة على هذا النوع من الشبكة
(الدش المركزي) فهو عبارة شبكة يرسل فيها أحد الاطراف بيانات إلى
الاطراف الاخرى التي تستقبل البيانات.

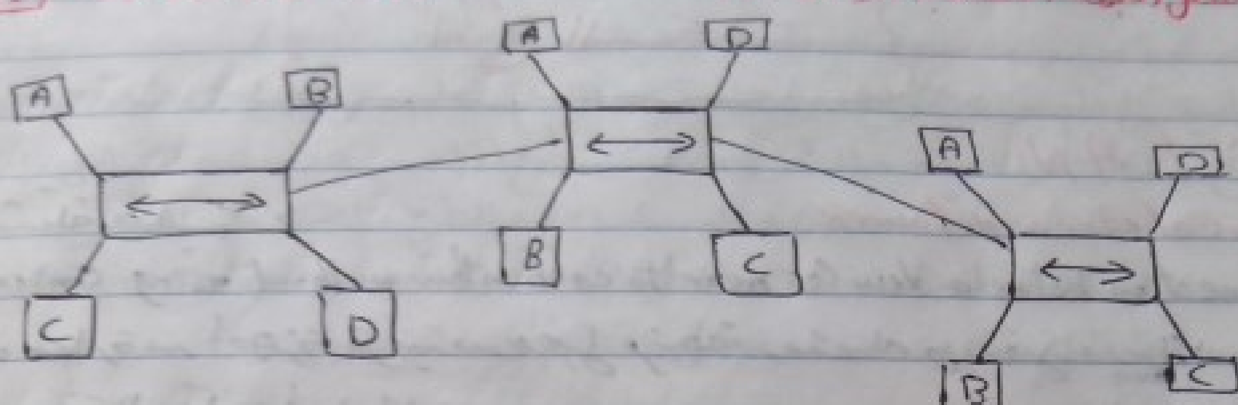
2 Star Topology   2 شكل النجمة



تتكون من نقطة مركزية متصل بها الاجهزة ليتكون في النهاية شكل الشبكة
(star)
هذا النوع هو الاكثر استخداما ولكن من عيوبه أنه إذا انقطعت النقطة المركزية
تسقط الشبكة جميعها.
في هذه الشبكة النقطة المركزية تستقبل البيانات من الطرف C مثلا ثم توجه
البيانات إلى الطرف B كما في الصورة.

* Transmission through a central point.

3 extended star — 3 شكل النجمة المتشعبة أو الممتدة

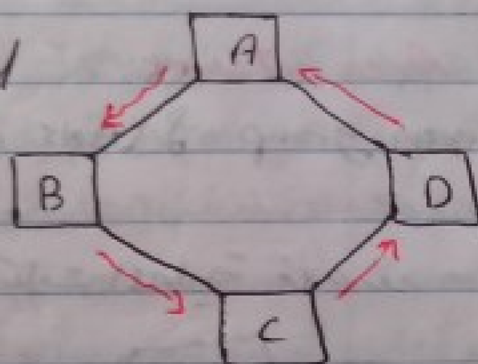


هي نفس فكرة star topology لكن بصورة متشعبة وممتدة.

More resilient than star topology أكثر مرونة من ستار توبولوجي

4 Token Ring Topology — 4 شكل الحلقة أو الدائرة.

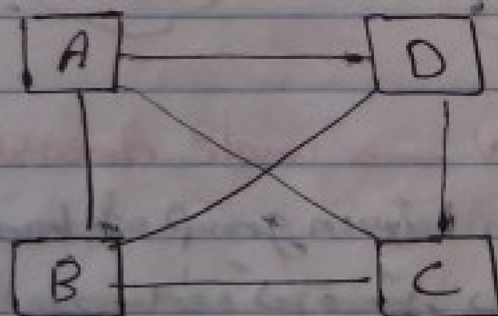
Signals travel around ring



طريقة توصيلها تكون على شكل حلقة ومن أهم عيوب Half duplex وهو
الإرسال يكون من اتجاه واحد وتكون بطيئة جداً

5 Mesh Topology

جميع الأطراف متصلة ببعضها البعض
عيوبها كثرة المشاكل وتكلفة
التنفيذ أو التطبيق



Highly Fault-tolerant
Expensive to implement

Network Types
أنواع الشبكات

① LAN

local Area Network — شبكة محلية.

Connection between devices near to each other without using central office

هي عبارة عن أجهزة قريبة من بعض ومرتبطة ومتصلة مع بعض دون الحاجة إلى سنترال مركزي أو ما شابه

غالباً تكون في حدود الـ ١٠ كيلومتر ويمكن أن يكون من الشبكة التي تستطيع انشائها بدون الاستفادة من أي طرف آخر مثل (ISP) internet service provider.

ومن شبكات المزودة لخدمة الانترنت مثل Te Data - link.

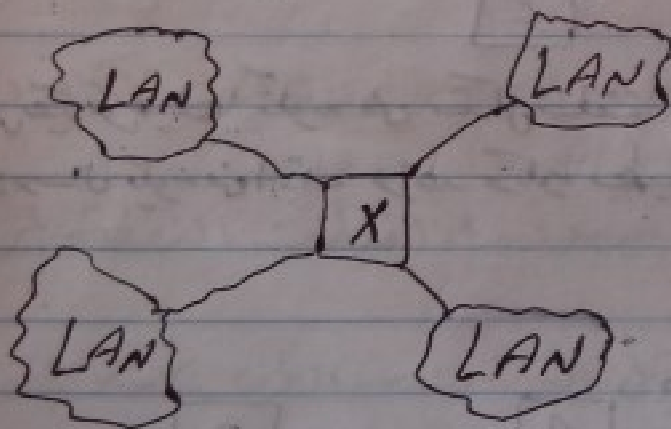
② Man

Metropolitan Area network — شبكة المستوى العاصمة

Connection between group of LANs over a small area within City like Cairo.

هي اتصال بين مجموعة من الشبكات المحلية في حدود مدينة مثل القاهرة

تستخدم فيها شركات ISP



[3] WAN → wide Area Network — شبكة المناطق البعيدة.

Connection between group of Lans over a large Area like Countries

اتصال بين مجموعة من الشبكات المحلية في حدود مناطق كبيرة مثل دولة ودولة أخرى

How Data Transfers

بداية كل علم وله قواعد يبني عليها هذا العلم فعلم الرياضيات مثلا يبنى على الجمع والطرح والقسمة والضرب فلا يستطيع الدارس دراسة التكامل والتفاضل وحساب المثلثات مثلا بدون دراسة الجمع والطرح والقسمة والضرب كذلك علم الشبكات يبنى على 7 طبقات (7 layer) سنقوم الآن بدراستها بصورة مختصرة قبل التكلم عنها بالتفصيل

OSI model "open System Interconnection"

بداية عملية نقل البيانات تمر بسبع مراحل أو طبقات من هذا النموذج وهي التي تظهر في الرسم.

pc①		pc②
Application	لكي تنتقل البيانات من الجهاز	Application
presentation	① إلى الجهاز رقم ② تمر بالطبقات	presentation
Session	المختلفة من الجهاز ① بدءا من	Session
Transport	Application ثم presentation	Transport
Network	ثم Session ... إلى physical	Network
Data link	ثم تنتقل الجهاز ② البيانات وتمر	Data link
physical	أيضا بنفس الطبقات لكن بالعكس	physical
	physical ثم Data link ثم ... Application	

~~① Application layer~~

why a layerd Network model ?

① Reduces Complexity — تقليل التعقيد

② Simplifies teaching and learning. — تسهيل التعلم وتبسيطه

① Application Layer.

used to represent a user interface to the network

باختصار هي البرامج التي يتعامل المستخدم مثل Browsing . yahoo msg. ع

② presentation Layer.

- Ensures that Data is Readable by receiving system قابلية القراءة
- Formats Data تهيئة البيانات
- Structure Data هيكلة البيانات
- Provides encryption تقوم بعملية التشفير

باختصار هي نفس طبقة Application كلمة presentation هي البيانات كيف يتم قراءتها من الكمبيوتر مثلاً فيلم على جهاز ما يقرأ كالتالي .... أي عملية تشفير للبيانات أي أن الفيلم يراه الشخص بصورة فيلم سينما يراه الجهاز نفسه كأرقام.

③ Session Layer.

- Interhost Communication تفتح قناة اتصال.
- Give order for: establishment of session
  - management of session
  - Termination of session

  → between source and destination.

  انشاء ← establishment, ادارة ← management, انهاء ← Termination.

Session قد تكون تفتح أو تحل

④ Transport Layer.

في هذه الطبقة يتم تقسيم الداتا إلى أجزاء " Segment ".

ويتم تسمية الداتا في هذه الطبقة إلى " Segment ".

في هذه الطبقة أيضاً يتم استخدام نوعين من النقل

Transmission Control protocol	User Datagram protocol.
TCP	UDP
	
reliable service موثوق بها	unreliable service غير موثوق بها
Sequenced متسلسل	unsequenced غير متسلسل.
~~Secure آمن~~	~~unsecure غير آمن~~
Connection oriented اتصال مباشر	Connection less دون اتصال مباشر
virtual Circuit دائرة ظاهرية	
ACK "acknowledgment" اشعار استلام	No ACK لا اشعار باستلام البيانات.

شرح الفرق بين TCP/UDP

باختصار كلاهما بروتوكول نقل البيانات كل منهما له مميزات أما هي.

١- TCP يضمن وصول البيانات بشكل سليم في حين أن ذلك غير مضمون في UDP

٢- TCP يرسل البيانات بشكل متسلسل مرتب في حين لا يرسل UDP بشكل متسلسل أو مرتب

٣- TCP ينشئ اتصال موجه أو اتصال مباشر أو ما يعرف دائرة ظاهرية بين المرسل والمستقبل بينما لا يقدم UDP هذه الخدمة.

٤- TCP حين يرسل segments تكون segments على شكل تسلسل ويستلم اشعار بالتوصيل أو الاستقبال من الطرف الآخر بناء عليه يتم ارسال الـ segment التالي وإذا لم يستلم ACK فلا يتم ارسال الـ segment التالي أما UDP فيتم ارسال الـ sequence دون انتظار أو التأكد من الاستقبال السليم لها.

٥- TCP أبطأ من UDP بسبب عملية التحقق والموثوقية التي تميزه عن UDP.

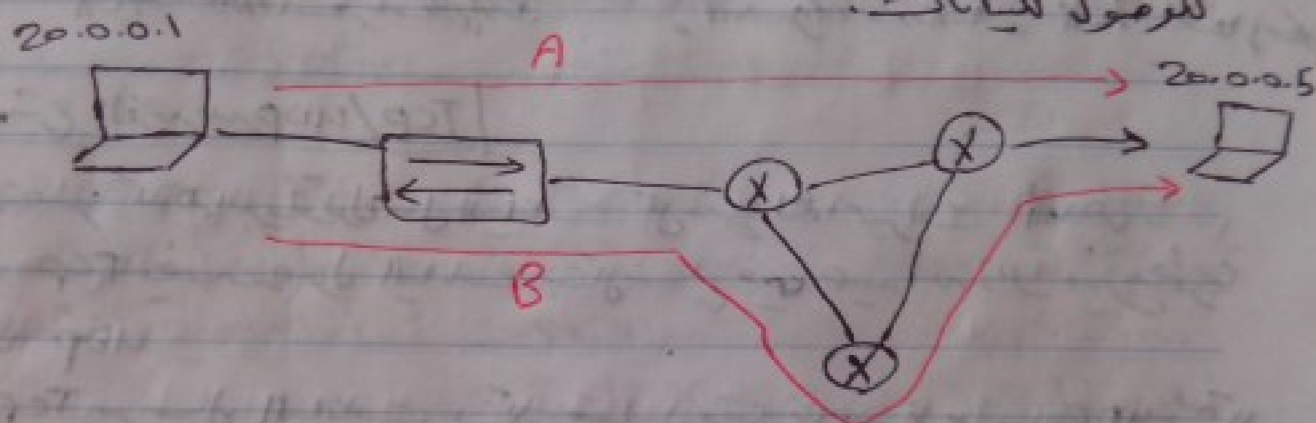
٦- من أوضح الأمثلة لـ TCP ← email بينما من أوضح الأمثلة لـ UDP هو البث المباشر.

⑤ Network Layer.

في هذه الطبقة يتم تسمية الداتا packets ومن هذه الطبقة يتم استخدام الراوتر الذي وظيفته توجيه واختيار أفضل طريق لنقل البيانات وأيضاً في هذه الطبقة يتم انشاء عنوان للمصدر source Ip وعنوان للمستقبل des. Ip

مثال

نفرض أن هناك جهاز هو source Ip رقم أو عنوانه 20.0.0.1 يرسل بيانات إلى des Ip رقم 20.0.0.5 كما بالرسم يظهر أكثر من طريق للوصول للبيانات.



في هذه الحالة يقوم الراوتر ⊗ باختيار أفضل الطرق وهو الطريق A حيث أنه به عدد أقل من الراوترات والتوصيلات من الطريق B فيظهر لنا في المثال دور الراوتر وهو اختيار أفضل الطرق.

الخلاصة لـ Network layer.

1. Routes Data packets — توجيه حزمة البيانات
2. Selects best path to deliver Data — اختيار أفضل الطرق للتوصيل
3. Provides logical addressing. — انشاء عنوان منطقية رقمية للمرسل أو إضافة والمستقبل النهائي.

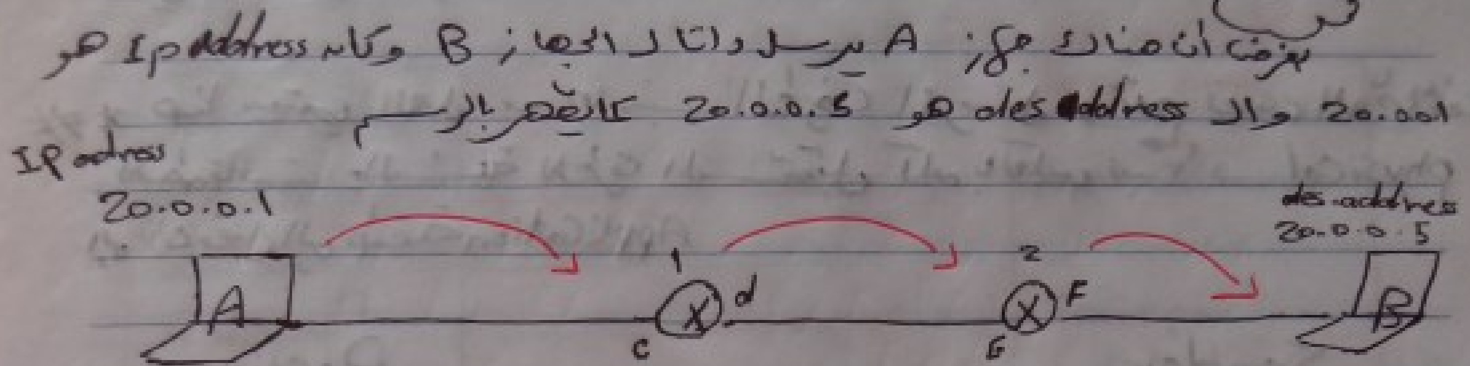
⑥ Datalink layer.

في هذه الطبقة يتم إضافة mac address وهو اختصار لكلمة media access Control ويسمى أيضاً physical address أي العنوان الحقيقي وهو مختلف عن Ip address في طبقة Network فهو عنوان logical وهي

مثال mac address بإختصار عنوان كرت الـ Lan أو رقم كرت الـ Lan الذي يميزه عن غيره من جميع الكروت الموجودة في العالم عادة يتكون من ١٢ رقم وحرف
ويتم تسمية الداتا في هذه الطبقة بـ Frame

مثال

نفرض أن هناك جهاز A يرسل داتا لـ الجهاز B وكان الـ Ip address هو 20.0.0.1 والـ des address هو 20.0.0.5 كما يظهر بالرسم



فحين يتم نقل البيانات لا يتغير كل من Ip address ولا حتى des address في حين أن الـ mac address يتغير فعند ارسال الداتا من الجهاز A إلى الراوتر الاول يكون الـ sourc mac address هو رقم الجهاز A ويكون الـ des. mac address هو المدخل c في الراوتر الاول ثم تخرج الداتا من الراوتر الاول فيكون src. mac address هو المخرج d ويكون des. mac. address هو المدخل E ثم تخرج الداتا من الراوتر الثاني من F وهو src. mac address إلى des. mac. address وهو الجهاز B
نفهم من ذلك أن Ip address و des. address لا يتغير في حين يتغير mac address عند خروج الداتا من الجهاز A ومرورها على الراوتر حيث أن الراوتر به كارت Lan مثل جهاز الكمبيوتر تماماً

- هذه العملية التي يضاف فيها عنوان الـ mac إلى الـ Frame وإزالته في كل مرة بين الراوتر والجهاز تسمى التغليف enCapsulation و de encapsulation نزع التغليف أي يتم اضافة عنوان الـ mac عند الانتقال من الجهاز للراوتر الاول ثم نزعها عند الوصول وحين يتم الارسال من الراوتر الاول للراوتر الثاني تحدث عملية جديدة من التغليف enCapsulation ثم لما تصل الداتا يتم نزع العنوان ولما تخرج من الراوتر الثاني إلى الجهاز B يتم اضافة en Capsulation.

الخلاصة

① Hop to Hop Data delivery.
② mac addressing
③ Hop to Hop error detection.
④ formating Data.

② physical Layer.

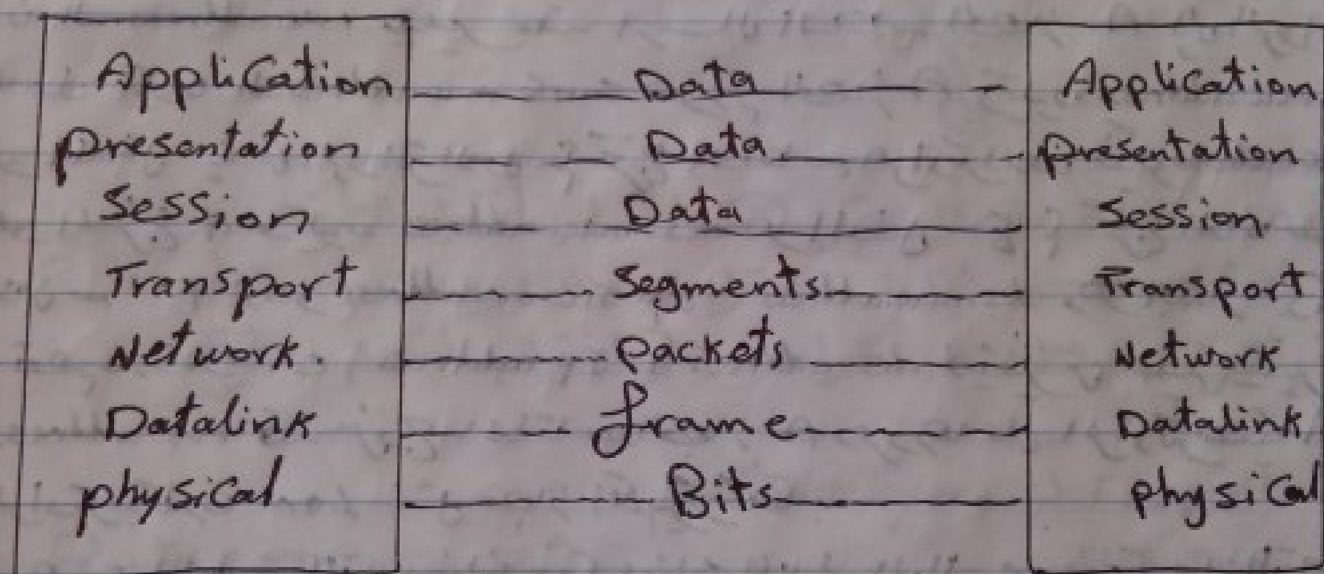
في هذه المرحلة أو الطبقة يتم تحويل الـ frame إلى Bits أو كهرباء وهي الطبقة المسؤولة عن جميع المعدات الفعلية للشبكة مثل أنواع الكابلات وكما سبق تحويل الداتا لكهرباء

* هنا ينتهي العمل من جانب الطرف المرسل وتتم نفس الوظائف للطبقات بالنسبة للطرف المستقبل لكنه بالعكس تبدأ من physical إلى أن تصل إلى طبقة Application

Sender | Receiver







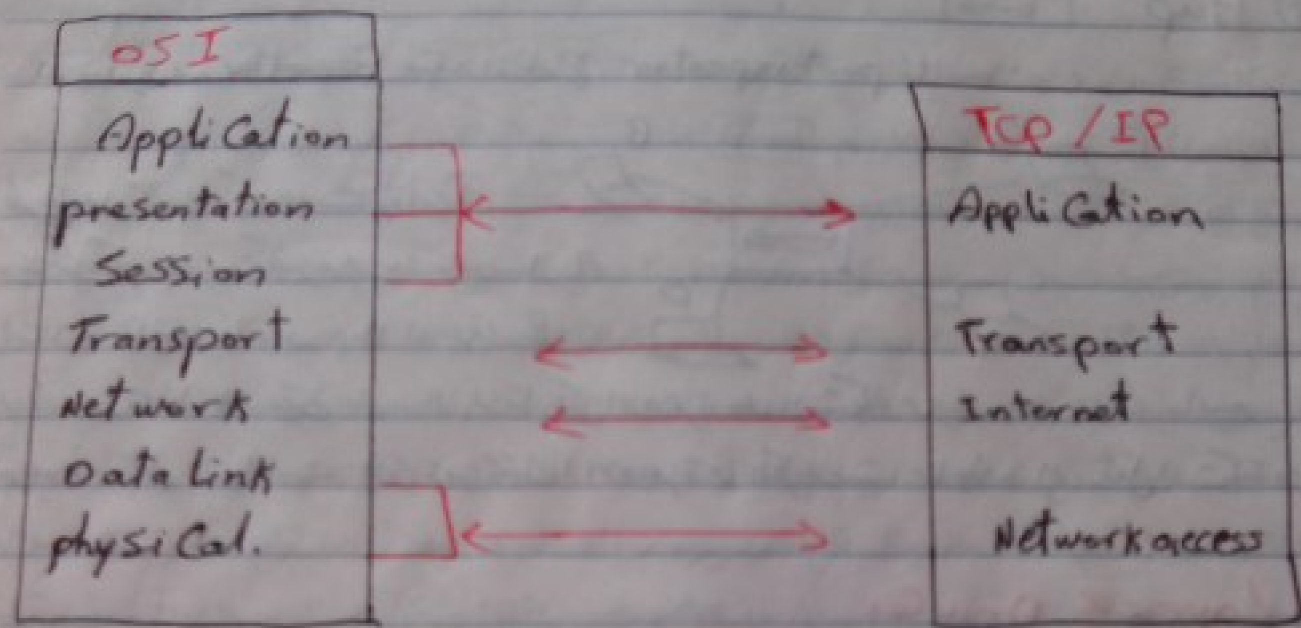
هام

العملية التي تمر بها البيانات في الجانب المرسل بداية من طبقة Application حتى تصل إلى physical تدعى عملية encapsulation التغليف

العملية التي تمر بها البيانات في الجانب المستقبل بداية من طبقة physical حتى طبقة Application هي عملية decapsulation.

TCP/IP "Transmission Control protocol / Internet protocol"

انشئ من قبل وزارة الدفاع الامريكية تتكون من ٤ طبقات



* يعد TCP/IP اكثر انتشاراً من OSI وذلك للاسباب

① flexible addressing scheme ① مرونة من حيث العنونة

② usability by most operating systems and platforms.

② قابلية الاستخدام من قبل معظم انظمة التشغيل والمنصات المختلفة

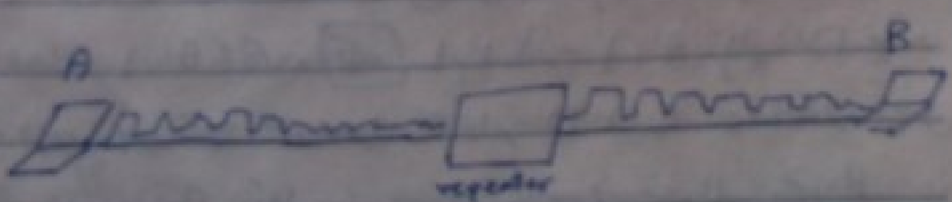
③ The need to use it to Connect to the internet.

Network Devices

① Layer 1 Devices

هي الاجهزة التي تتحكم في الطبقة الاولى "physical layer"

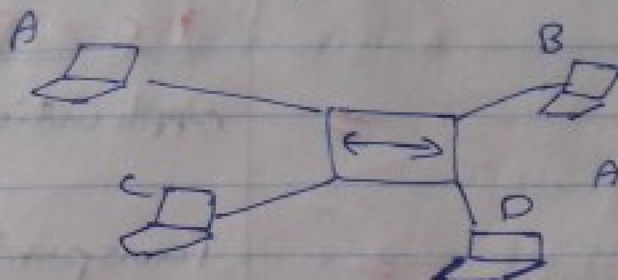
① Repeater



وظيفة الـ Repeater هو أنه يكرر الاشارة ويقويها حيث أنه كابلات النت
يكون مسافتها ١٠٠ متر وبعدها تضعف الاشارة.

② Hup

هو عبارة عن Repeater متعدد المخارج أو multi port repeater



طريقة عمل Hup يكرر الاشارة أيضاً ويقويها لكنه به عيباً كبير وهو عندما يرسل A داتا لـ B مثلاً نجد الـ Hup لا يعرف B من أي بورت لذلك يقوم بارسال الداتا لكل الاجهزة على الشبكة مما يؤدي إلى حدوث ما يسمى Loop وهو أنه تظل البيانات التي لم يستقبلها الاجهزة في الكابلات مما يؤدي إلى ثقل الشبكة وبطئها.

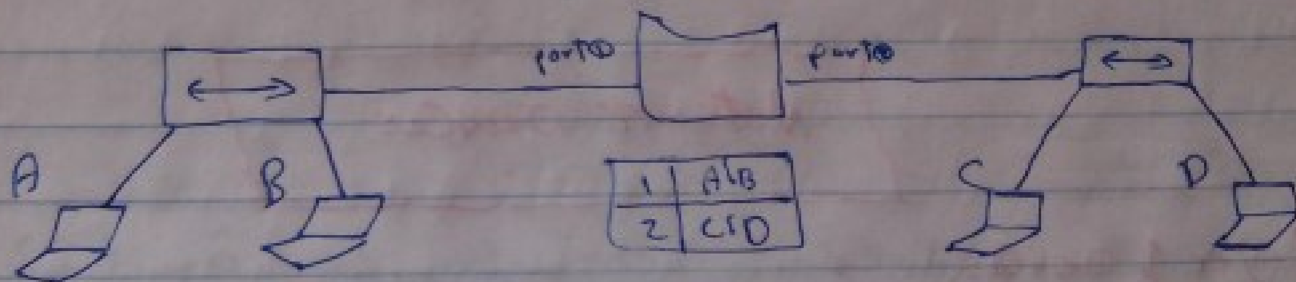
② Layer 2 Devices

هي الاجهزة التي تستخدم في الطبقة الثانية "Data link layer".

① NIC "Network interface Card" كارت الشبكة

2 Bridge

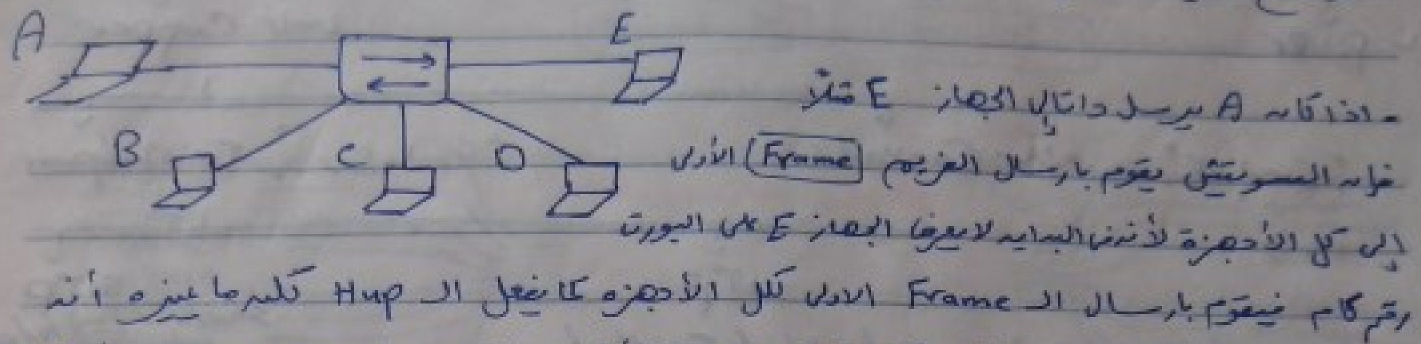
Bridge تعني جسر وتتضح طريقة عمله من الشكل



إذا كان A يرسل داتا إلى B فإن الـ Bridge لا يمرر الاشارة إلى الأجهزة على البورت ٢ وهي C,D وكذلك إذا كان C يرسل داتا إلى D فإنه لا يمرر الاشارة إلى الاجهزة على البورت ١ A,B. لكن إذا أرسل A إلى D فإنه Bridge يقوم بتمرير الاشارة إلى البورت ٢ للوصول للجهاز C,D فبالتالي تصل إلى الجهاز المراد D أي أن الـ Bridge يقلل من Loop وهي عيوب الـ Hup

3 Switch

يتميز بكفاءة وسرعة أعلى من Bridge وبه عدد مخارج أكثر من Bridge
وتتضح فكرة عمله من المثال



- اذا كان A يرسل داتا إلى الجهاز E مثلا
فإن السويتش يقوم بإرسال الفريم (Frame) الأول
إلى كل الأجهزة لأنه في البداية لا يعرف الجهاز E على أي البورت
رقم كام فيقوم بإرسال الـ Frame الأول لكل الأجهزة كما يفعل الـ Hup لكن ما يميزه أنه
يسجل الـ macaddress الخاص بكل جهاز والبورت الخاص به في جدول يسمى Cam table
أو يسمى أيضا mac address table فعند بداية تشغيل الـ switch يكون هذا الجدول فارغ
فعند ارسال أول Frame يسجل الـ mac الخاص بالـ src السورس وهو الجهاز A
في المثال ويرسل الـ Frame لكل الاجهزة ويرد فقط الجهاز المستلم وهو E في المثال
فيسجل الـ mac الخاص به على أي بورت في switch وهكذا في كل عملية ارسال إلى أن يكتمل
الجدول لديه بعدها لو أرسل A إلى D مثلا تخرج الداتا من A إلى D فقط
وبالتالي تقل حدوث الـ Loop

وطريقة عمل الجدول

A	port ①	[illegible]	
B	port ②	D	port ④
C	port ③	G	port ⑤

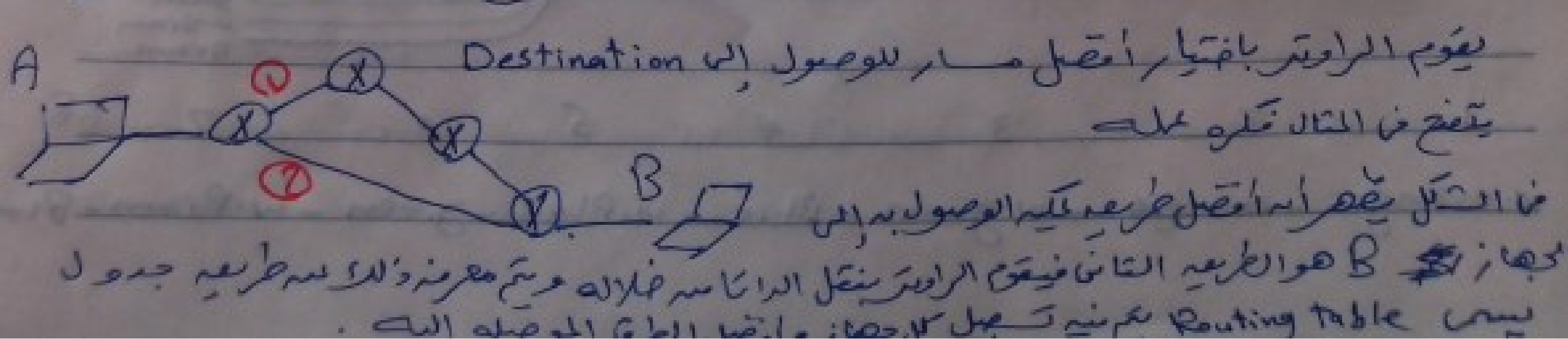
الجدول يسجل به الـ mac الخاص بالمرسل والمستقبل في
كل عملية إلى أن يكتمل الجدول عندئذ لا يتم ارسال الداتا
لكل أطراف الشبكة لكن لمن ارسلت إليه فقط لأنه تم تسجيل المخرج الذي يجب أن
تخرج الداتا منه للوصول للجهاز المطلوب

3 Layer 3 DeviCes

هي الأجهزة التي تستخدم في الطبقة الثالثة "Network layer"

1 Router (X)

يقوم الراوتر باختيار أفضل مسار للوصول إلى Destination
يتضح في المثال فكرة عمله



في الشكل يظهر أن أفضل طريق لكي الوصول به إلى
الجهاز B هو الطريق الثاني فيقوم الراوتر بنقل الداتا منه خلاله ويتم معرفة ذلك من طريق جدول
يسمى Routing Table يتم فيه تسجيل كل الأجهزة وأفضل الطرق الموصلة إليه.

The Cables

Fiber فايبر

Copper نحاس

Coaxail سلك محوري ، كابل ترسي

Twisted pair ؛ زوج ملتوفات

UTP
Unshielded Twisted pair زوج ملتوفا غير محمي

STP
Shielded Twisted pair
زوج ملتوفا محمي

لمعرفة التوصيلات نوضح ذلك في الجدول

1	2
pc Router	Hup Switch

① اذا وصلنا أي جهاز من العمود ① بأي جهاز من العمود ② نستخدم وصله Straight

② اذا وصلنا أي جهاز من ① بجهاز من نفس العمود أو جهاز من ② بجهاز من نفس العمود
تكون الوصله اسمها Crossover

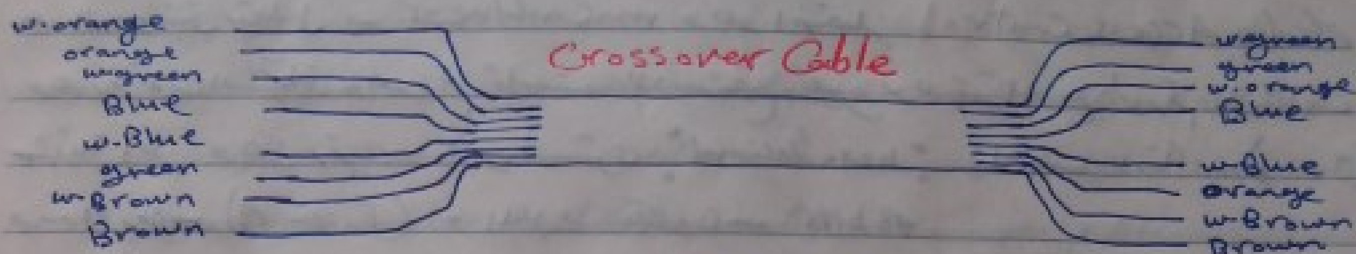


1 2 3 4 5 6 7 8

w.orange _ orange _ w.green _ Blue _ w.Blue _ green _ w.Brown _ Brown

② Crossover Cable

في هذه الوصلة يكون أحد الطرفين نفس وصلة الـ straight من حيث الترتيب والطرف الآخر يتم استبدال اللون الأبيض البرتقالي والبرتقالي بالأبيض الأخضر والأخضر بمعنى آخر تم استبدال الـ [1 مكان 3] و [2 مكان 6]



يكون طرف مثل وصلة straight
والطرف الآخر يكون بترتيب آخر كالتالي

3	6	1	4	5	2	7	8
w.green	green	w.orange	Bule	w.Blue	orange	w.Brown	Brown

تنبيهات

١- كابلات Twistedpair تنقسم إلى
- Cat5 ← أقل سرعة ١٠ ميجا
- Cat5e ← أعلى سرعة ١٠٠ ميجا
- Cat6 ← سرعة بالجيجا

٢- الاسم العلمي Twistedpair ← Base T أيضا

٣- Cat5 يعمل بـ ميزة ethernet ، Cat5e ← ميزة Fastethernet
Cat6 ← Gigaethernet

٤- أقصى مسافة للكابل هي ١٠٠ متر وبعدها الإشارة تضعف ونحتاج Repeater أو سويتش

Switching

السويتش من الاجزاء المتعبه التي يتم التعامل معها يوميا فالتعامل مع السويتش يكون أكثر من التعامل مع الراوتر

* السويتش يتعامل ب mac address وهو اختصار Media Access Control وهو رقم كرت الشبكة وهو رقم ثابت لا استطيع تغيره ولا يتشابه مع اي رقم على كارت شبكة آخر وهو رقم سداسي عشري hexadecimal يتكون من الارقام من (٠ ← ٩) ومن الحروف من (A ← F) والماك مكون من 48 bits .

* السويتش هو Layer 2 ومعنى ذلك انه لا يفهم ال Ip ولكنه يفهم ال Layer 2 OSI
* للحصول على رقم ال mac address ← نكتب الامر Ip Config /all يظهر لنا اسم الماك ويكون اسمه physical address ويكون مكون من ١٦ رقم وحرفا
* ال mac address لا يمكن أن يتشابه مع رقم كرت آخر ولا استطيع تغيره وبالتالي عند توصيل أجهزة الكمبيوتر بالسويتش يتواصل معها ويعرف الماك الخاص بكل جهاز عن طريق بروتوكول ARP

ARP protocol

بروتوكول ARP هو اختصار Address Resolution Protocol ووظيفته هو الذي يتواصل مع جهاز الكمبيوتر يعرف ال mac address الخاص به ويسجله في switching table الخاص بالسويتش و ال Switching table هو الذي يميز السويتش عن ال Hup فال Hup لا يعرف ال mac address وبالتالي يرسل الداتا لكل الاجهزه مما يؤدي إلى حدوث ما يسمى Loop لكن السويتش يسجل الماك الخاص بكل جهاز في Switching table ويقوم بعمليه تسجيل ومعرفة الماك ببروتوكول ARP وبالتالي عند ارسال الداتا يرسل السويتش من Source إلى ال Destination ولا يتم ارسال الداتا لكل الأجهزة.

* عند توصيل السويتش بأجهزة الكمبيوتر يعمل السويتش مباشرة بعد مرور ٣٠ ثانية
في أثناء الـ ٣٠ ثانية يمر بمراحل هي
① Listening ← مدتها ١٥ ثانية في هذه المرحلة يبدأ في التعرف على الأجهزة.
② Learning ← مدتها ١٥ ثانية في هذه المرحلة يبدأ في تسجيل الـ macaddress
بعد المرحلتين ندخل في مرحلة الـ Forward وهي مرحلة الإرسال والاستقبال.

* تكون السويتش في الغالب ٢٤ بورت تنقسم هذه البورتات أصبحت أنواع تختلف السرعة
فهناك منافذ تكون ← ethernet ← ١٠ ميجا / ثانية
منافذ ← Fast ethernet ← ١٠٠ ميجا / ثانية
منافذ ← Giga ethernet ← ١ جيجا

Switch Configuration

للتعرف على الأوامر التي عن طريقها نستطيع عمل Configuration للسويتش لابد أن أعرف
الـ modes الخاصة بالسويتش

Switch mode

Switch > enable	User mode
Switch #	privileged mode
Switch (config) #	Global Configuration mode
Switch (config-if) #	Interface mode
Switch (config-subif) #	Subinterface mode
Switch (config-line) #	Line mode

* عند عملية إجراء الـ Configuration للسويتش يتم توصيل السويتش بجهاز الكمبيوتر بوصلة Console
متصلة في الكمبيوتر بـ السيريال بورت [.....] وبالسويتش في بورت ethernet

* لتفعيل السويتش والانتقال الـ Privileged

switch > en or enable

switch # ——> privileged mode

* للانتقال من privileged إلى global config.

switch # config t

switch (config) # ——> global configuration

* للانتقال من global config إلى Submode وكيله interface

switch (config) # Interface Fo/—— رقم البورت

switch (config-if) # ——> Subinterface mode

* للعودة من أي mode إلى الـ mode السابعه نستخدم edit أو Ctrl+Z

مهم: عند وضع استفهام ? عند كل mode يساعد ذلك في معرفة الاوامر المتاحه في هذا المود

switch > ?

Some Command for Switch

الآن سنتعرف على بعض الاوامر التي نستطيع من خلالها التحكم في السويتش

① تغيير اسم السويتش

Switch>en

switch # Config T

Switch (config) # hostname Ahmed (or) host Ahmed

② عمل حماية على الـ Console

وصلة الـ Console هي الوصلة التي يتم توصيلها بين الجهاز الكمبيوتر وبين السويتش لإعطاء الأوامر للسويتش.

نستطيع التحكم في هذه الناحية عن طريق بعض الأوامر التي تساعدنا في التحكم في استخدام الـ Console لإجراء الـ Configuration

Switch > en

Switch # Config T

Switch (Config) # Line Console 0

Switch (Config-line) # password [123] باسورد هي ١٢٣

Switch (Config-line) # login تفعيل الباسورد

Switch (Config-line) # exec-timeout 5 7 تحديد وقت تفعيل الباسورد وبعدها ينتهي

وهو ٥ دقائق و٧ ثواني كما في المثال لو تركناها (0 0) لا ينتهي الباسورد أبداً

③ عمل حماية لـ privileged mode

يتم أيضاً التحكم في الـ privileged عن طريق عمل حماية لها

Switch > en

Switch # Config T

Switch (Config) # enable secret 123 باسورد مشفرة

أو

Switch (Config) # enable password 123 باسورد غير مشفرة

وللإلغاء الباسورد نضيف كلمة [No] قبل الأمر نفسه

Switch (Config) # No enable secret (or) Switch (Config) # No enable password

④ التحكم في سرعة الـ Port

يمكننا أيضاً التحكم في سرعة البورت حيث أن سرعة البورت إما ١٠ ميجا / ثانية "ethernet" أو تكون السرعة ١٠٠ ميجا / ثانية "Fast ethernet" أو تكون السرعة بالجيجا "Giga ethernet". لكن يمكننا التحكم في سرعة البورت أي يمكن أصبح تقليل السرعة حيث أنه فعلياً طبعاً لا يمكن زيادة السرعة عن السرعة الفعلية للبورت

وللتحكم في سرعة البورت نستخدم الاوامر التالية

```
switch >en
switch # Config t
switch(config)# interface F0/1
switch(config-if)# Speed 10
switch(config-if)# speed ?
switch(config-if)# speed Auto
```

البورت 0/1

حددنا السرعة بـ ١٠ ميجا/ثانية

لمعرفة الاوامر المتاحة للسرعة ويظهر لنا إما ١٠ ميجا/ثانية أو ١٠٠ ميجا/ثانية أو Auto وهي السرعة الطبيعية للبورت

اعادة السرعة لـ Default الاصلية

⑤ خاصية الـ Full Duplex و خاصية الـ Half Duplex

لفهم عمل الـ Full Duplex والـ Half Duplex لابد أن نعرف أن كابل UTP مكون من ٨ كابلات يستخدم البني والابيض البني كباور ويتبقى ٦ كابلات وهي تستخدم في النقل لكن المستخدم فعلياً يكون ٤ كابلات وهذا فقط في خاصية الـ Half Duplex وهي عبارة عن أن الهوست يكون إما مستقبل أو مرسل لا يمكن أن يكون مرسل ومستقبل في نفس الوقت لأن ذلك يؤدي إلى حدوث تصادم للداتا Collision لذلك تم انشاء بروتوكول CSMA/CD

CSMA/CD protocol

بروتوكول الـ CSMA/CD هو اختصار

Carrier Sence Multiple access / Collision Detection

يعمل هذا البروتوكول فقط في وضع الـ Half Duplex ووظيفته عبارة عن منظم لعملية ارسال الداتا يقوم بعرض من أرسل الداتا أولاً ثم يقوم بالسماح لها بالمرور ثم يتعرف على الداتا المستقبلة ويتم السماح لها بالمرور في الوقت الذي لا يكون فيه داتا أخرى تم ارسالها أي أنه يمنع عملية تصادم الداتا حتى لا تتم فقد أي جزء منها لأن الداتا في Half Duplex تمر خلال كابل واحد فيقوم البروتوكول بتنظيم عملية نقلها لمنع التصادم

* وضع Full Duplex
في هذا الوضع يكون النقل خلال ٦ كابلات وليس ٤ كابلات كما Half Duplex
في هذا الوضع يكون هناك كابل للارسال وكابل للاستقبال وبالتالي لا يحدث تصادم
للداتا وبالتالي لا نحتاج لبروتوكول CSMA / CD في هذا الوضع

اعداد خاصيه Full Duplex وال Half Duplex

```
Switch > en
Switch # Config T
Switch (Config) # interface Fa0/1
Switch (config-if) # Duplex half      وضع ال Half
                     Duplex Full      وضع ال Full
                     Duplex Auto      وضع ال Auto
```

* في حالة اذا تم تغيير وضع ال Duplex في السويتش إلى وضع ال Full Duplex فان كارت الشبكة المتصل بالسويتش والخاص بجهاز الكمبيوتر يتحول أيضا إلى ال Full Duplex مباشرة
كل هذا لا يتم في برنامج ال packet Tracer حيث لا يتم ذلك بشكل اوتوماتيك حيث نضطر إلى تعديل كارت الشبكة الخاص بجهاز الكمبيوتر من حالة Auto Duplex إلى حالة Full Deplex يدويا

⑦ إنشاء ⇐ Banner
البانر عبارة عن رساله أو بيانات يمكن اضافتها للسويتش لتوضيح معلومة أو رساله ترحيب أو رسالة تحذير وينقسم البانر إلى ثلاثة اقسام

Banner exec	Banner Login	Banner Motd
يظهر في كل الاحوال وداخل أدائما لفترة معينة	لا يظهر إلا في وجود باسورد مطلوب	(Massage of The Day رسالة يومية

• إنشاء Banner motd

Switch>en

Switch # Config T

Switch(config) # Banner motd # Hello #

ونلاحظ تكتب الرسالة بين علامتين غريبتين مثل مثل علامة الدولار هكذا $

Switchport modes

ينقسم المود الخاص بالبورت في السويتش إلى Access و Trunk

- البورت الذي يتصل به جهاز كمبيوتر يسمى Access
- البورت الذي يتصل به جهاز سويتش آخر يسمى Trunk
- عند توصيل جهاز الكمبيوتر بالسويتش يتعرف السويتش على البورت تلقائياً أنه Access

لكن في بعض الأحيان لابد من إعطاء الأمر للسويتش لكي يتعرف على البورت أنه Access
ونفس الأمر في حالة Trunk

• لجعل السويتش يقرأ البورت على أنه Access أو Trunk

Switch>en

Switch # Config T

Switch(Config) # int Fa/1

Switch(config-if)# switchport ~~Acess~~ mode Access

Switch(config-if)# switchport mode Trunk

لمعرفة هل طبقه للأمر أو لا نستخدم أمر show run سيظهر هل طبقه أم لا

Switch# show Run

port Security

هي خاصية هامة جدًا عن طريقها يتم التحكم في البورت من اكتشاف الانتهاكات التي تتم على البورت ولنفهم ذلك تعرفنا أنه شخص ما على الشبكة أزال الجهاز المتصل على الشبكة في العمل مثلاً وأتى بجهاز آخر ولكنه اللابتوب الخاص به وقام بتوصيله بالكابل الخاص بالجهاز الأصلي الذي أزاله من الشبكة في هذه الحالة قد يقوم هذا المستخدم بفعل أي شيء يضر بالشبكة أو حتى يزيل الشبكة نفسها دون العلم من قام بذلك فلكي نتفادى هذه المشكلة نستخدم port security وهي باختصار لو تم تغيير الماك الخاص بجهاز الكمبيوتر المتصل بالسويتش يقوم السويتش بإغلاق البورت حتى لو قام الشخص بإعادة الجهاز الأصلي الذي به الـ mac address المتعرف عليه من قبل السويتش فإن السويتش لن يفتح البورت مرة ثانية إلا من خلال الأدمن ← تلك هي فكرة الـ port Security

* تفعيل خاصية الـ port Security

[١] تحديد البورت على أساس أنه Access

```
Switch(Config)# int Fo/1
Switch (config-if)# Switchport mode Access
```

* بفرض أنه أكثر من بورت في شكل متتالية نستخدم أمر Range

مثل
```
Switch(config)# int range Fo/1 - 5
Switch (config-if-range)# Switchport mode Access
```

* بفرض أنه أكثر من بورت لكنه غير متتالية

مثل
```
Switch (config)# int range Fo/1 , Fo/3 , Fo/5
Switch (config-if-range)# Switchport mode Access
```

[٢] استدعاء خاصية الـ port security

```
Switch (config-if)# Switchport port-security
```

[٣] تحديد الماك المراد تثبيته وحفظه

```
Switch (config-if)# switchport port-security mac address ___ex___
```

لكن يعيب هذه الخطوة رقم [٣] أنه قد يحدث فيها خطأ عند تثبيت الماك حيث أنه بفرض عدد الأجهزة من ٢٠٠ إلى ٣٠٠ جهاز قد يؤدي ذلك إلى خطأ في عنوان رقم Mac معين ولذلك نستطيع تجنب هذا الخطأ عن طريق أمر يجعل السويتش يحفظ أول ماك تم توصيله بالبورت وهو الأمر sticky

مشكلة أخرى من هذه الخطوة الثالثة وهي كيفية الاتيان بـ macaddress فأنا نستطيع معرفة الـ mac عن طريق أمر Ip Config /all ويسمى الـ physical address أو من بعد عن طريق الأمر getmac /s ip

← أي عنوان الـ Ip الخاص بالجهاز المراد معرفة الماك الخاص به

لكي نختصر الطريقة الثالثة نستخدم الأمر Sticky

```
switch (config-if) # switchport port-security mac address sticky
```

إذا أردنا حفظ أكثر من ماك جهاز

```
switch (config) # int range Fo/1-3
switch (config-if-range) # switchport mode Access
switch (config-if-range) # switchport port-security macaddress sticky
```

(هام) عند قيام أحد ما باستبدال الجهاز الذي تم تسجيل الماك الخاص به على البورت فإن السويتش يغلق البورت تماماً حتى لو قام الشخص بإعادة الجهاز الأصلي سيظل البورت مغلق ولإعادة تشغيل البورت نتبع الآتي مثلاً

```
switch (config) # int range Fo/2-3
switch (config-if-range) # shutdown
switch (config-if-range) # No shutdown
```

بهذه الطريقة يرجع البورت إلى العمل بحالته الأصلية.

(هام) لمعرفة البورت المفعل على خاصية الـ port security والتي تم اكتشاف اختراق نستخدم الأمر show

```
switch # show port-security address
```

خاصية ال Mac address Maximum

هي خاصية عن طريقها نستطيع البورت قراءة أكثر من macaddress على نفس البورت

مثال

أجهزة (Voip) وهي عبارة عن أجهزة تليفونية تأخذ عنوان Ip بالإضافة إلى أنه يتم توصيلها بالسويتش من ناحية ومن الأخرى يتم توصيلها بالكمبيوتر كما بالرسم



في هذه الحالة البورت متصل عليه أكثر من Mac وهم الماك الخاص بالهاتف والماك الخاص بجهاز الكمبيوتر فنستطيع أن نجعل البورت يقرأ كلا الماكين أو أكثر عن طريق استخدام خاصية ال Macaddress maximum

مثلا switch (config-if) # switch port port-security maximum 2

switch (config-if) switch port port-security mac address ___ ex

ولإضافة الماك الثاني نعيد الأمر ونكتب الماك الثاني وهنا الزيادة عن 2 يمنع على البورت.

خاصية Violation

كلمة Violation تعني انتهاك أو اختراق والمراد هنا الإجراءات التي تتخذ عند حدوث عملية اختراق للبورت أو استبدال للجهاز المعرف على البورت في هذه الحالة يكون هنالك ثلاث اجراءات

Shutdown	protect	Restrict
⇓	⇓	⇓
يتم اغلاق البورت عند استبدال الجهاز حتى ولو تم إعادة الجهاز الأصلي فإن البورت سيظل مغلق حتى يقوم الأدمن بفتحه مرة أخرى وهي الخاصية ال Default	يتم اغلاق البورت عند استبدال الجهاز لكن حين يتم إعادة الجهاز الأصلي فإن البورت سيعود للعمل بصورة طبيعية دون رسالة إنذار للأدمن بحدوث اختراق	نفس فكرة عمل ال protect لكن مع ارسال رسالة للأدمن بحدوث اختراق

لتفعيل ال protect أو Restrict

switch(config-if)#switchport port-security violation protect/Restrict mode

port security خلاصة الـ

① التعامل مع بورت واحد

```
Switch >en
Switch # Config T
Switch (Config) # int Fo/1                                      (تحديد البورت)
Switch (Config-if) # Switchport mode access                     (تحديد المود)
Switch (Config-if) # Switchport port-security                   (استعداد الخاصية)
Switch (Config-if) # Switchport port-security macaddress ___    تفعيل الخاصية على ماك معين
```

أو تفعل أمر sticky مكان الخطوة الأخيرة

```
Switch(Config-if) # Switchport port-security macaddress sticky                تفعيلها
Switch (Config-if) # Switchport port-security maximum 3     مثلاً              خاصية maximum
Switch (Config-if) # Switchport port-security macaddress ___ ...
Switch (Config-if) # Switchport port-security voilation shutdown
Switch (Config-if) # exit                                      خاصية الـ voilation
Switch (Config) # exit
Switch # show port-security address                             لعرض البورت المفعل عليه الخاصية.
```

② للتعامل مع أكثر من بورت

```
Switch >en
Switch # Config t
Switch (Config) # int range Fo/1-5                               لو متتالية
Switch (Config) # int range Fo/1, Fo/3, Fo/5                     لو غير متتالية
Switch (Config-if-range) # Switchport mode Access                تحديد المود
Switch (Config-if-range) # Switchport port-security              استعداد الخاصية
Switch (Config-if-range) # Switchport port-security macaddress sticky
Switch (Config-if-range) # Switchport port-security maximum 3    مثلاً
Switch (Config-if-range) # Switchport port-security voilation shutdown mode
Switch (Config-if-range) # exit
Switch (Config) # exit
Switch # show port-security address
```

عند جعل Shutdown للبورت ونريد عمل فتحه مرة أخرى

switch > en
Switch # Config t
Switch (config) # int F0/1 — نحدد البورت
Switch (Config-iF) # shutdown — نعمل shutdown وبعدها
Switch (Config-iF) # No Shutdown — نعمل No shutdown

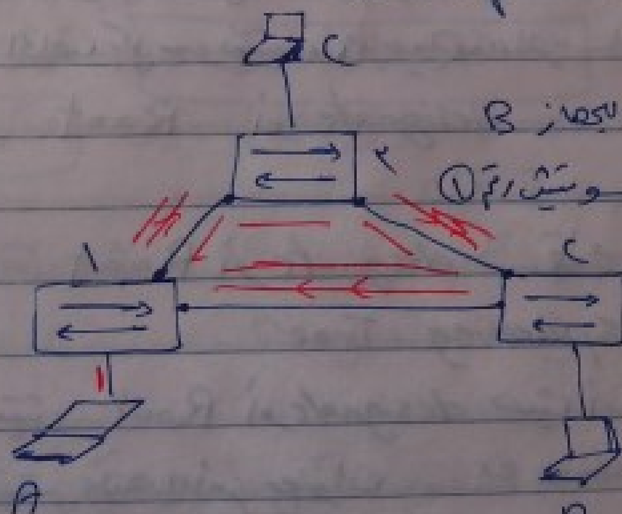
Spanning Tree protocol

STP

هو واحد اشهر بروتوكولات الـ Switching وله أيضاً اسم آخر وهو اسم علمي له وهو 802.1d

ويعد بروتوكول STP هو بروتوكول خاص بسيسكو يعمل في وجود سويتشين أو أكثر وهو يعمل بصورة أوتوماتيكية وهو يعمل على تقليل حدوث عملية اللوب "Loop avoidance".

مثال لفهم عملية الـ Loop



بفرض أن الجهاز A يرسل داتا للجهاز B
فإن الداتا تخرج من A إلى السويتش رقم ① الذي يقوم بإرسالها للسويتش رقم ② والسويتش رقم ③ ورقم ③ يرسلها إلى B ورقم ② يرسلها إلى C

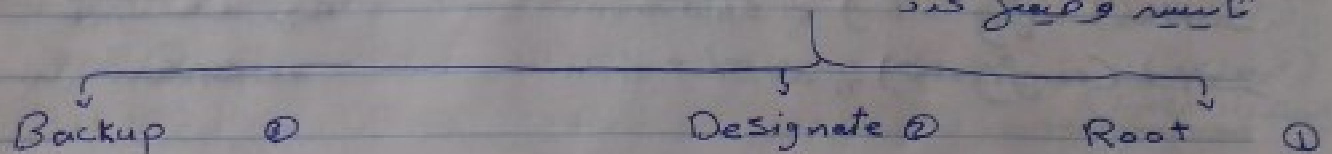
فعند إجراء كل إرسال يتبقى جزء من الداتا في الكابلات مما يؤدي إلى ثقل الشبكة وهو ما يعرف بعملية الـ Loop.

في المثال وضح أنه يوجد أكثر من طريق لتوصيل الداتا لكن وجود أكثر من طريق يؤدي لحدوث Loop فيقوم STP بتفعيل طريق واحد وجعل الثاني بديل في حالة حدوث تلف أو عطل وبذلك نتلاشى أو نقلل

في الشبكة مثل الـ Loop

خاصية الـ Bpdu

هي اختصار Bridge protocol Data unit وهي عبارة عن رسالة يتم ارسالها كل ثانيتين ووظيفتها تحدد



ولفهم هذه المصطلحات نوضح مثال

بفرض أننا نضم مبنى من ٤ أدوار يوجد سويتش مركزي في الداتا سنتر يكون سويتش مركزي ليس Root الأدوار الأخرى لا أستطيع أن أمد كابلات للأجهزة في كل دور بالجهاز الـ Root مباشرة لكن لازم أن يكون في كل دور من المبنى سويتش خادم لهذا الدور ويتم توصيل هذا السويتش " designate " بالجهاز المركزي وهو الـ Root وهكذا في كل أدوار المبنى.

وظيفة الـ Bpdu هي ارسال رسالة كل ثانيتين يقوم بارسالها كل سويتش لكي يحصل على الـ mac address الخاص بكل سويتش عن طريق هذه الرسالة يستطيع السويتش أن يحدد دوره هل هو Root أو designate

- ولمعرفة هل السويتش Root أو designate نستخدم الأمر show

switch # show spanning - Tree

سيظهر لنا هل السويتش Root أو designate حيث أنه يظهر الماك الخاص بالسويتش الذي نفذت عليه الأمر بعنوان ex ـــ Bridge ID Address

ويظهر الجهاز الـ Root بعنوان ⟵ Root ID

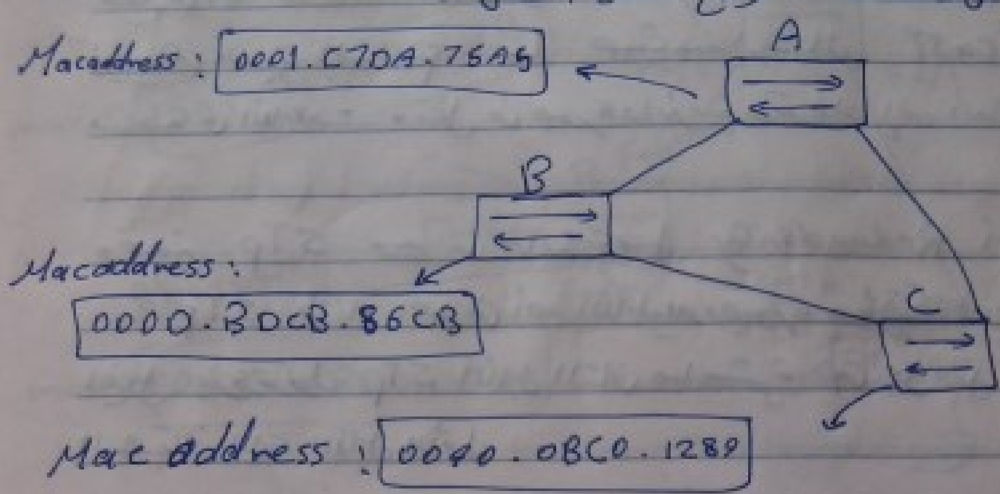
ويكون الماك الخاص به هو ـــ ex ـــ لكن بفرض أني نفذت الامر على جهاز الـ Root ستظهر لي رسالة تؤكد أن الجهاز هو الـ Root

وسنلاحظ أن Root Id Address & BridgeID Address بنفس العنوان ـــ ex

* كيفية تحديد الجهاز الـ Root و Designate

يتم اختيار الجهاز الـ Root على أساس أنه صاحب أقل Mac Address

ولمعرفة أقل ماك Macaddress نوضح المثال التالي.



نلاحظ في المثال أن السويتش A عنوان الماك الخاص به يبدأ 0001 مجموعهم 1 + صفر + صفر + صفر = 1 ونلاحظ أن الجهاز B عنوان الماك يبدأ 0000 فنقوم بتحويل الـ D إلى 13 حيث أن رقم الماك هو رقم سداسي عشري hexadecimal

F E D C B A
15 14 13 12 11 10 9 8 7 6 5 4 3 2 1

فنجد أن D مقابلها 13 فيكون عنوان الماك الخاص بالسويتش B = 13 + صفر + صفر + صفر = 13 فيكون A أقل من B وبالنسبة للجهاز C عنوان الماك الخاص به هو 0040 فيكون صفر + 4 + صفر + صفر = 4 فيكون أيضاً A أقل من B و C

لذلك يكون الجهاز A هو الجهاز الـ Root والأجهزة B و C هي الأجهزة الـ Designate

(هام) هذه الرسالة Bpdu تقوم بشكل أوتوماتيكي بتحديد من هو الجهاز الـ Root ومن الـ Designate وعندما ينتهي تحديد من هو الروت Root لا تقوم السويتشات الأخرى بإرسال رسالة الـ Bpdu ويقوم جهاز الـ Root فقط بإرسال هذه الرسالة كل ثانيتين لتعريف باقي الأجهزة أنه هو الروت ويحتوي الرسالة على الماك الخاص به

خاصية الـ Redundancy

كلمة Redundancy هي الوفرة أو الزيادة عن الحاجة
باختصار هي زيادة في عدد الكابلات عن الحاجة بغرض تأمين الشبكة في حالة
قطع في أحد الكابلات أو تعرضه للتلف ولكن كانت هذه ميزة لكنها تؤدي إلى عيب
كبير وهو حدوث الـ Loop حيث عند إرسال Broadcast يتم إرسال
نسخة في الكابلات وتظل في صورة دائرية وتتردد إلى أن تتعرض الشبكة للبطء والضياع

وضعنا STP ⇐ في حالة توصيل Redundancy أي أكثر من كابل يقوم بروتوكول
STP بإلغاء العمل في أحد الكابلين بصورة مؤقتة وفي حالة تعرضه لأي تلف
تفعل بروتوكول STP الكابل الثاني مباشرة حتى يحل محل الكابل التالف فلا تتأثر
الشبكة بتلف الكابل الأول

لفهم هذه العملية لابد أن نوضح أمور
١- Root ⇐ وهو الجهاز صاحب أقل Mac address وهو الذي شرحناه سابقًا
٢- designate ⇐ هي كل الأجهزة الأخرى غير الـ Root وتسمى Non-Root Bridge
٣- كل البورتات على جهاز الروت تسمى Forward port وأيضا "designated port"
٤- Root port ← وهو بورت يكون في الجهاز الـ Designate ويكون صاحب أقرب طريق
ذو أقل تكلفة للجهاز الروت أي التي تكون مرتبطة معه
٥- ← إذا كان لدى أكثر من لينك multilink يقوم الـ STP ← باختيار Root port
واحد من اللينكات وطريقة الاختيار تكون اختيار أقل شيء في ① cost ② port number (رقم البورت)

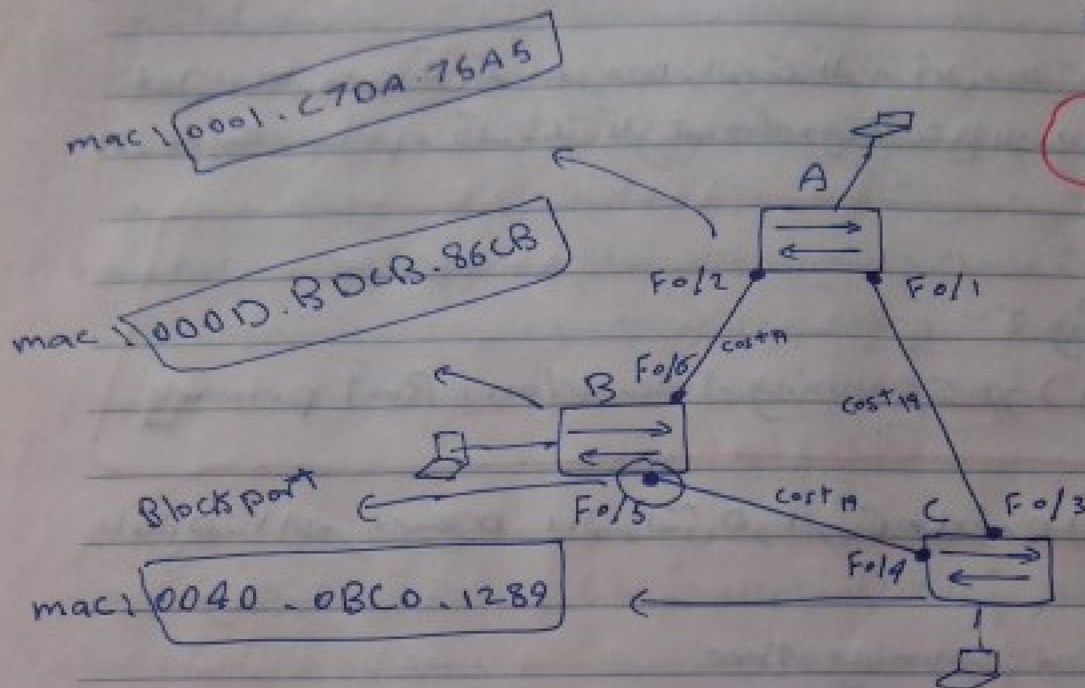
بالنسبة للـ Cost وهي التكلفة	
Speed	Cost
10G	2
G.E	٤
F.E	19
E	١٠٠

بالنسبة لرقم البورت
F0/1
F0/2
F0/3

إذا كان الحساب أي حساب التكلفة لوصول بورتات السويتش الـ Designate

متساوي ننتقل إلى حساب أقل رقم للبورت وصاحب الرقم الأقل يكون هو الـ Rootport

مثال شامل



حل هذا المثال

١- جهاز الـ Root هو الجهاز A ⇐ صاحب أقل mac كما بينا في المثال السابق

٢- Designated أو Forward port هي البورتات Fo/1 و Fo/2 لأنها بورتات الجهاز الـ Root

٣- Rootport الخاص بالجهاز C هو البورت Fo/3 لأنه صاحب أقل تكلفة في الوصول إلى الجهاز الروت

٤- الـ Rootport الخاص بالجهاز B هو البورت Fo/6 لأنه صاحب أقل تكلفة في الوصول للجهاز الـ Root

٥- Designatedport الخاص بالوصلة بين السويتش B و C هو صاحب أقل ماك واتضح لنا أن أقل ماك هو C فيكون Fo/4 هو DP أو الـ Designatedport

٦- Blocks port ⇐ وهو البورت الأخير الذي ليس RP أو Rootport ولا DP أو Designatedport ويكون هو البورت Fo/5

* هذا المثال يوضح فكرة عمل الـ STP والإجابة تعمل بشكل تلقائي.

إجبار سويتش معين على أن يكون هو ال Root

لجعل جهاز معين لكي يكون هو جهاز الروت لكونه أعلى من حيث الامكانيات ومخارج ال ethernet به أعلى من غيره مثلاً كلها Giga ethernet نتبع الاوامر التالية

```
switch>en
switch# Config T
switch(Config)# Spanning-Tree Vlan 1 Root primary
```

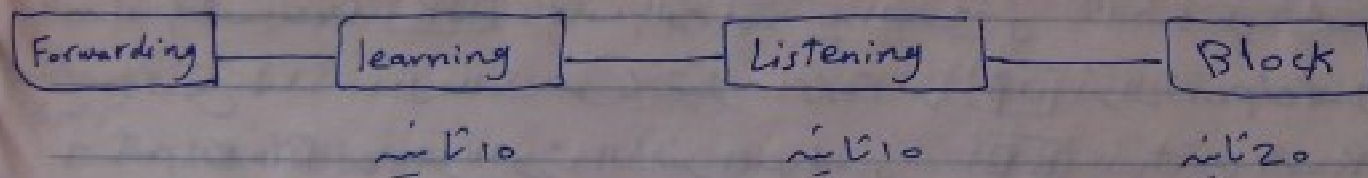
باتباع هذا الامر يصبح هذا السويتش هو الروت ولمعرفة هل أصبح الروت ولا لا

```
switch>en
switch# show spanning-tree
```

سيظهر لنا انه أصبح هو الجهاز ال Root

خاصية ال Rapid pvst

وضحنا في عملية ال Redundancy أنه الكابل التالف يقوم بروتوكول STP باستبدال العمل على الكابل البديل لكن عملية الاستبدال يتم فيها بعض التأخير حيث أنها تمر بعدة مراحل تأخذ حوالي ٥٠ ثانية مقسمة إلى



بعد مرور حوالي ٥٠ ثانية يعمل الكابل البديل مكان الكابل التالف لكن هذه المدة في عالم الشبكات والعمل قد تؤدي إلى مشاكل ولكي نتفادى هذه المشاكل نستخدم خاصية Rapid-pvst التي تجعل الكابل يعمل مكان الكابل التالف مباشرة دون انتظار ٥٠ ثانية ولكي نفعل هذه الخاصية نتبع الامر الآتي في كل أجهزة السويتش سواء ال الجهاز ال Root أو الاجهزة الأخرى ال Designate

خاصية الـ Rapid-pvst

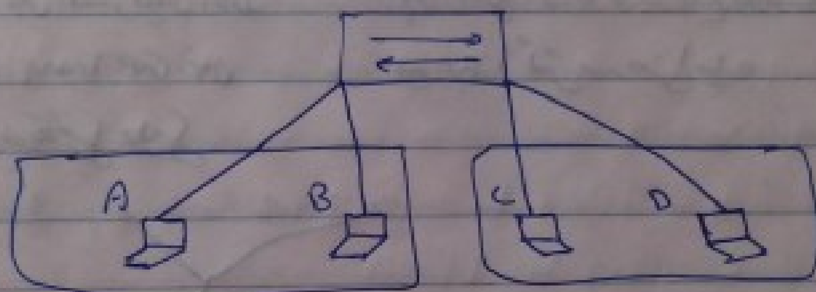
```
switch>en
Switch# Config T
Switch(Config)# Spanning-Tree mode Rapid-pvst
```

ونفعل الامر على كل السويتشات لانه إذا كان هناك احد السويتشات على الوضع العادي pvst فإن الجميع سيعمل على هذا الوضع ولتفعيل الوضع السريع لابد أن تفعل rapid-pvst على كل السويتشات.

VLAN

الـ VLAN هو اختصار Virtual LAN أي شبكات داخلية وهمية

فكرة عمل الـ VLAN تتضح من المثال التالي:



تقوم الـ VLAN على امكانية اعتبار الجهازين A/B شبكة منفصلة عن الجهازين C/D فإذا أرسل A داتا سيستقبلها B فقط وإذا أرسل C داتا سيستقبلها D فقط، رغم أنهم جميعًا مشتركين في سويتش واحد

فوائد الـ VLAN

١- تقلل عملية الـ Loop

٢- عملية الاضافة بكفاءة عالية " أكثر منه Subnet " أي تقسم الأجهزة لشبكات مختلفة

٣- حل مشكلة physical limitation يعني لو كان السويتش مليان فأقدر أشبك شخص تابع لنفس القسم في سويتش آخر وأربطه معهم

٤- أستطيع تجميع أجهزة قسم معين في VLAN واحده حتى لو كانوا في اماكن مختلفة أو سويتشات مختلفة

ملاحظة: عند شراء السويتش تكون جميع بورتات السويتش موجودة في VLAN1 الموجودة على السويتش فإذا أردنا أن ننشئ VLAN جديدة نبدأ من VLAN2 ونستطيع إنشاء حتى 4096 VLAN والسبب أننا إذا وصلنا أجهزة على سويتش فإن جميع الأجهزة تستطيع أن ترى بعضها البعض لأن كلها تحت الـ VLAN1 التي موجودة أصلاً على الجهاز فإذا أنشأنا أكثر من VLAN نستطيع التحكم فيمن يستطيع رؤية الآخر حسب كل جهاز موقعه في VLAN أولاً.

البروتوكولات الخاصة بالـ VLAN

802.1Q

هو البروتوكول الأكثر شيوعاً ويعمل على منافذ الـ Trunk حيث يقوم البروتوكول بتعريف بيانات الـ VLAN على السويتش الأول وتخرج من منافذ الـ Trunk حتى تصل إلى السويتشات الأخرى وتعرف عليها.

ISL "Inter switching Layer"

هو بروتوكول وإنه كان خاص بشركة سيسكو إلا أنه الآن لا ننصح باستخدامه حيث أنه عيوبه أكثر من مزاياه

هذه البروتوكولات تعمل بصورة أوتوماتيكية

* لمعرفة الـ VLAN الموجودة على السويتش نستخدم الأمر show

```
switch > en
switch# show VLAN
```

قبل إنشاء أي VLAN ستظهر لنا الـ Default VLAN وهي VLAN1 ومهمتها تجعل جميع الأجهزة المتصلة على السويتش ترى بعضها البعض لذلك ستظهر لنا وسيظهر أن جميع البورتات على السويتش مدرجة تحت هذه الـ VLAN1

VLAN Configuration

تمر عملية إنشاء الـ VLAN بعدة مراحل

[١-] تحدد عنوان للشبكة أي لكل VLAN مثل ⟸ [192.10.10.0]

[٢-] تحدد Ip الأجهزة تحت أي عنوان VLAN مثل [192.10.10.1] ده Ip الـ pc1

[٣-] أوامر السويتش

① إنشاء VLAN
② تسمية الـ VLAN
③ تحديد البورتات الـ Access
④ تحديد البورتات الـ Trunk
⑤ ادراج المخارج الخاصه بالأجهزة تحت كل VLAN خاصة بها

① إنشاء الـ VLAN

```
Switch>en
Switch#Config T
Switch(config)#VLAN 2
```
مثلا

② تسمية الـ VLAN

```
Switch>en
Switch#Config T
Switch(config)#VLAN 2
Switch(Config-VLAN)#Name Accounting
```
مثلا

③ تحديد البورتات الـ Access

```
switch>en
Switch# Config_T
Switch(config)# int Fo/1
Switch(config-if)# switchport mode Access
```

في حالة أكثر من بورت متتالي

مثلاً

```
switch(config)# int range Fo/1-4
switch(config-if-range)# Switchport mode Access
```

في حالة أكثر من بورت غير متتالية

مثلاً

```
Switch(config)# int range Fo/1, Fo/3, Fo/5
Switch(config-if-range)# switchport mode Access
```

④ تحديد للخارج Trunk

```
switch>en
Switch# Config T
Switch(config)#int Fo/1      مثلاً
switch(config-if)# switchport mode Trunk
```

وفي حالة كانت أكثر من بورت سواء متتالي أو غير متتالي نستخدم الـ Range كما في بورتات الـ Access

⑤ ادراج البورتات الخاصة بالأجهزة تبع كل VLAN خاصة بكل جهاز

```
Switch>en
switch# Config T
Switch(config)# VLAN 2          ← انشاء
Switch(config-vlan)# Name Accounting     تسمية
Switch(config-vlan)# exit
Switch(config)# int Fo/1      مثلاً
```

تحديد البورت تبع أي VLAN

switch(config)# int Fo/1
switch(config-if)# switchport Access VLAN2

حددنا البورت Fo/1 تابع للـ VLAN2

في حالة أكثر من بورت متتالي

switch(config)# int range Fo/1-4
switch(config-if-range)# switchport Access VLAN2

حددنا البورتات من 1 إلى 4 تبع الـ VLAN4

في حالة أكثر من بورت غير متتالي

switch(config)# int range Fo/1, Fo/3, Fo/5
switch(config-if-range)# switchport Access VLAN2

حددنا البورتات 1، 3، 5 تبع الـ VLAN2

بعض الأوامر الأخرى

- لمعرفة الـ VLAN الموجودة على السويتش وأي بورت تبع أي VLAN ⟸ show

switch>en
switch# show VLAN

- لمعرفة البورتات التي تقف عليها أمر الـ Trunk

switch# show interfaces Trunk

- لمعرفة خصائص كل بورت نستخدم الأمر Showrun

switch# showrun

سيظهر كل بورت تبع أي VLAN

- لإضافة وصفاً "description" لأي بورت

1- نحدد البورت

switch(config)# int Fo/1

2- نكتب الوصف

switch(config-if)# description Connected to VLAN2

switch(config-if)# exit

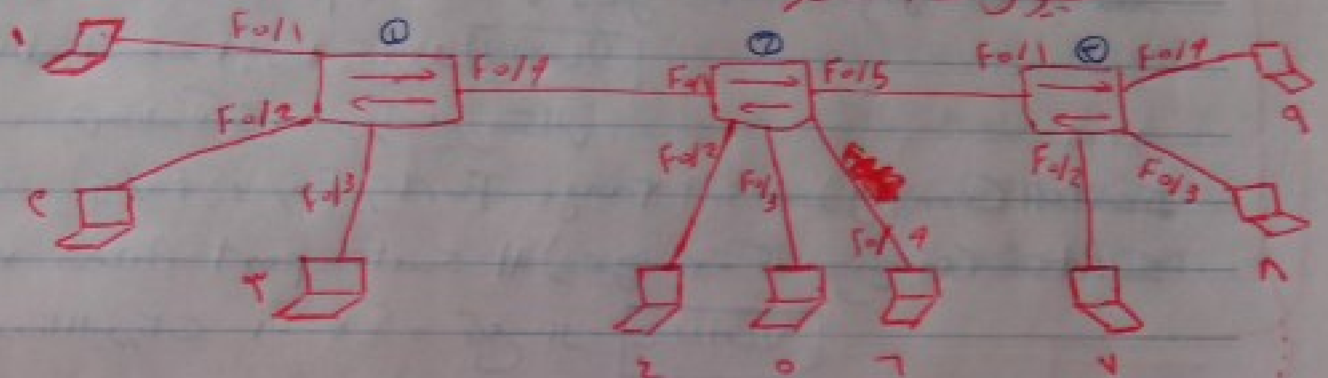
مثال ↖

لو عملنا أمر show run

switch # show run

سيظهر لنا البورت ومكتوب تحته الوصف الذي تم اضافته عليه وهو Connected To VLAN3 كما في المثال السابق

(مثال) شبكة مكونة من ٣ أجهزة سويتش ومتصل بكل سويتش ٣ أجهزة كمبيوتر كما بالصورة



يريد صاحب الاجهزة أن يجعل الاجهزة ١ و ٣ و ٨ في الـ Accounting والاجهزة ٢ و ٤ و ٥ في الـ Sales والأجهزة ٦ و ٧ و ٩ في IT والمطلوب الآن إنشاء الـ VLANs لإتمام هذه المهمة.

(الاجابه)

أولاً وضح من المثال أننا سوف نقوم بإنشاء ٣ من الـ VLANs وهي

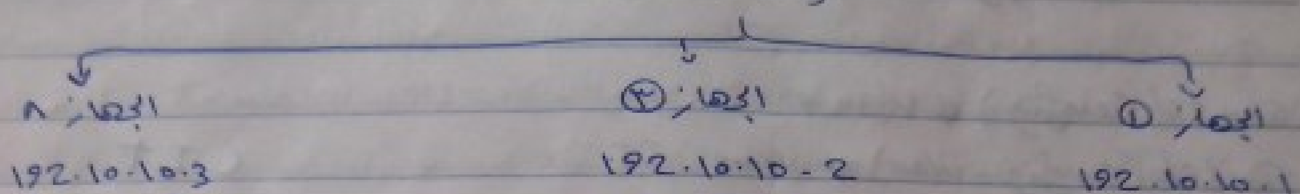
① Accounting ② Sales ③ IT

[1] تحديد عنوان لكل VLAN

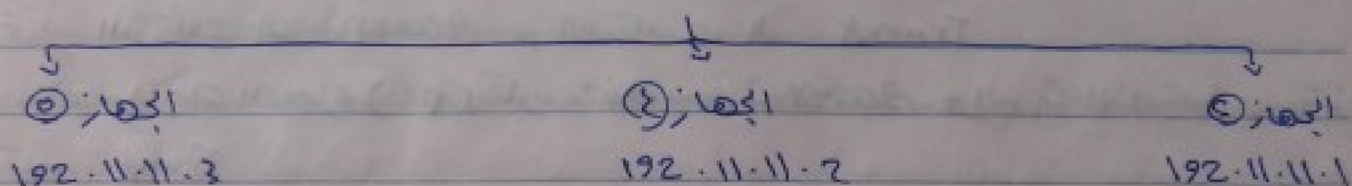
- Accounting 192.10.10.0
- Sales 192.11.11.0
- IT 192.12.12.0

ج اعطاء أجهزة كل VLAN ← IP من الشبكة الخاصة بها

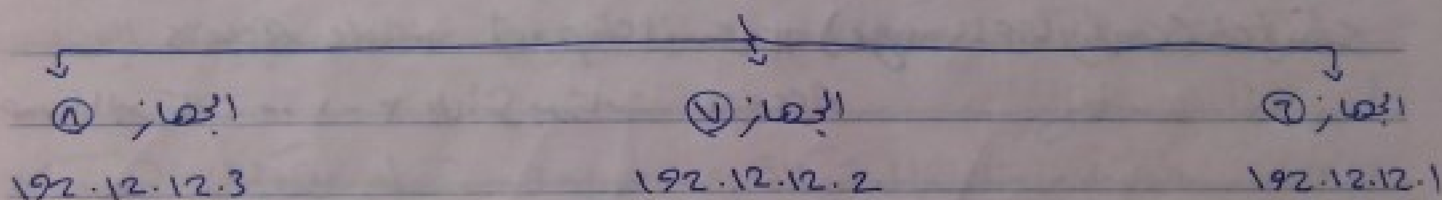
Accounting



Sales



IT



٣ أوامر الـ Configuration الخاصة بكل سويتش

- الجهاز ١

```
Switch > en
switch # Config T
Switch(config)#
```

انشاء وتسمية الـ VLANs

```
switch(Config) # VLAN 2
Switch(config-vLAN)# Name accounting        (Accounting)
Switch(config-vlan) # exit
```

Switch(config)# VLAN 3
Switch (config-vlan)# Name Sales (Sales)
Switch (config-vlan)# exit

Switch(config)# vlan 4
Switch (config-vlan)# Name IT (IT)
Switch (config-vlan)# exit

* تحديد البورتات الـ Access و البورتات الـ Trunk
في هذه المرحلة الاجهزة (PC) تكون متصلة ببورتات Access والبورت الذي يتصل بسويتش تكون Trunk

Switch(config)# int range Fo/1-3
Switch(config-if-range)# switchport mode Access
حددنا البورتات من ١ - ٣ على انها بورتات Access

Switch(config)# int Fo/4
Switch(config-if)# Switchport mode Trunk
حددنا البورت Fo/4 على أنه ⇐ Trunk

* ادراج كل بورت تحت الـ VLAN المخصصة له

Switch (config)# int range Fo/1, Fo/3
Switch (config-if-range)# Switchport Access VLAN 2
حددنا البورت Fo/1 ، Fo/3 تبع VLAN2 وهي الـ Accounting

Switch(config)# int Fo/2
Switch (config-if)# switchport Access VLAN3
حددنا البورت Fo/2 تبع VLAN3 وهي الـ Sales

انتهينا من الـ Configuration الخاصة بالسويتش رقم واحد (1)

* بالنسبة للسويتش رقم 2، 3 نتبع نفس الخطوات

① ننشئ الـ VLANs ونسميها.

② نحدد البورتات الـ Access والبورتات الـ Trunk

③ ندرج كل بورت تحت الـ VLAN الخاصة به

ولمعرفة ما تم انشائه على السويتش نستخدم الأمر

switch # show vlans

سيوضح هذا الأمر الـ VLANs وأسمائها والبورتات الخاصة بكل VLAN

(ملاحظة) في هذا المثال لابد لنا أن نقوم بعملية الـ Configuration على كل جهاز من أجهزة السويتش لكن هذه العملية قد تكون متعبة وشاقة نظراً لاختلاف اماكن السويتشات وقد يؤدي تكرار الـ Configuration إلى نسيان أو الخطأ في بعضها

لذلك نستطيع تلافي تلك المشكلة عن طريق استخدام بروتوكول VTP

VTP

بروتوكول الـ VTP هو اختصار ← VLAN Trunking protocol

وهو بروتوكول خاص بسيسكو وفكرة عمله باختصار هو أنه عند انشاء Configuration على سويتش معين يقوم هذا البروتوكول عند تفعيله بإنشاء نسخة من الـ VLAN Configuration على باقي السويتشات مما يوفر الجهد والوقت.

وبالرغم من انه يوفر بعض المزايا إلا أن سيسكو تنصح بعدم استخدامه نظراً لأنه لو حدث خطأ في الـ Configuration في السويتش سيقوم هذا البروتوكول بعمل نسخ من الـ Configuration بما فيها الخطأ ونسخه على باقي أجهزة السويتش

* تفعيل بروتوكول VTP

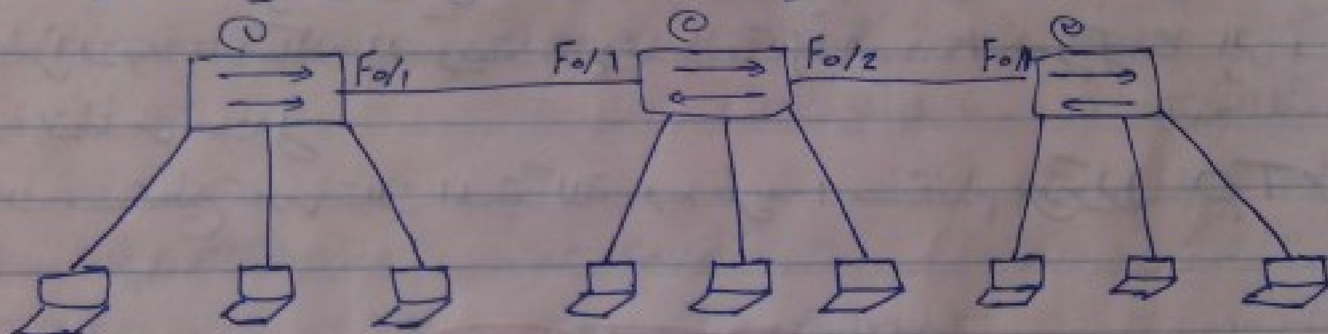
① تعريف البورتات التي تربط السويتشات مع بعض على أنها Trunk

② إنشاء Domin ويكون بنفس الاسم على كل السويتشات وإنشاء كلمة سر على كل السويتشات

③ تحديد جهاز واحد على أنه الجهاز ال Server وهو الذي تم إنشاء كل ال VLAN عليه

شرح العناصر السابقة بالتفصيل

① تعريف البورتات على أنها Trunk ونقصد بها التي تربط بين السويتشات




```
Switch>en
switch# ConfigT
Switch(Config)# int Fo/1
switch(config-if)#switchport mode Trunk
```

حددنا البورت Fo/1 الذي يربط السويتش ① بالسويتش ② على أنه Trunk
ونفعل نفس الخطوة من كل البورتات التي تربط بين أجهزة السويتش وبعضها البعض ونعرفها على أنها بورتات Trunk

⑥ إنشاء Domin باسم معين وإنشاء كلمة سر

قبل أن نبدأ في فهم هذه الخطوة لابد أن نعرف أننا إذا كتبنا أمر
switch # show VTp status
يظهر لنا بعض المعلومات الخاصة ببروتوكول VTP من ضمنها

VTp operating mode	: Server
VTp Domin Name	: فارغة

سنوضح هذه النقطة في الفقرة التالية

نلاحظ أن الDominName فارغ ولكي نقوم بتفعيل بروتوكول VTP لابد أن نحدد Domin name ونضع له كلمة سر حتى لا يستطيع أن أحد أن ينسخ ال Configuration إلى أي سويتش جديد إلا بعد إدخال كلمة السر

* إنشاء ال Domainname وكلمة السر.

```
switch >en
switch #config T
Switch (config) # VTp mode Server
switch (config) # VTp domin Ahmed
Switch (config) # VTP password 1234
```

(هام) عند انشاء ال Domin وضحنا أنه يكون في البداية Dominename فارغ لكن عند تسميته بأي اسم تقوم السويتشات الأخرى بالانضمام لذلك ال Domin مباشرة
يعني لو أننا نفذنا أمر switch # show VTp Status
على السويتش الثاني أو الثالث في المثال السابق نجد الصورة كالتالي
VTp operating mode : Server
VTP Domin Name : Ahmed
أي أنه سحب ال Dominname وانضم ليه بمجرد إنشائه لأنه في الأصل فارغ فلما وجد أنه تم انشاء Domin قبل السويتش الانضمام إليه بدل من أن يكون فارغ

③ تحديد الجهاز الذي تم إنشاء الـ VLANs عليه على أنه الـ Server والباقي من أجهزة السويتش client

لفهم هذا الامر لابد أن نفرق بين الـ server و client و Transparent

VTp modes of operation

Server	Client	Transparent
- كل أجهزة السويتش من سيسكو في البداية تكون على وضع server	- لا نستطيع إنشاء - حذف - اضافة أو اعادة تسمية على الـ VLANs من خلاله	- توصي شركة سيسكو بأن نجعل الأجهزة على هذا الـ mode
- تستطيع من خلاله إنشاء - حذف - إضافة - اعادة تسمية الـ VLANS	- لا يحفظ الـ VLAN وتعديلاتها على NVRam كداتابيز	- لديه المقدرة على حفظ الـ Vlan على nvRam
- يحفظ الـ VLAN وتعديلاتها على NVRam كداتابيز	- مجرد مستقبل يقوم بتمرير البيانات دون إجراء أي تعديل عليها وتحدث هذه البيانات تغيرات عليه	- البيانات التي يتم إنشاؤها عليه لا يتم نشرها إلى جيرانه ولكن المعلومات التي يستقبلها يرسلها.
- يعمل نسخة من الـ VLAN وتعديلاتها ويمررها للأجهزة الأخرى		

بعد أن فهمنا الفرق بين client و server و Transparent

لابد أن نجعل جهاز واحد server وهو الجهاز الذي نقوم بإنشاء الـ Vlans عليه والباقي client

* خطوات جعل الجهاز server

```
switch > en
switch # Config T
switch(config)# VTp mode server
```

ملاحظة وضع سيرفر هو الوضع ال Default وعلى الا افتح انه اعمل على الجهاز الانشاءات عليه ال VLAN

* خطوات جعل الجهاز Client وتفعيل ال Domin و ال password

```
switch > en
switch # Config T
switch(config) # VTp mode client
Switch (Config) # VTp Domin Ahmed
Switch (config) # VTp password 1239
```

مثلا

بعد الخطوات التالية

١- انشاء الConfiguration الخاصة بـ مود Trunk للبورت بين السويتشات

٢- إنشاء ال Dominname والباسوورد

٣- تعريف ٢ switch على أنه client

← لو عملنا أمر Show Vlan تظهر ال VLAN على السويتش ١ على الجهاز رقم ٢ لأننا فعلنا ال VTp

الخلاصة

يتضح لنا أنه وظيفة VTp هي إنشاء ال VLAN على السويتشات الأخرى بعد اتباع الخطوات السابقة.

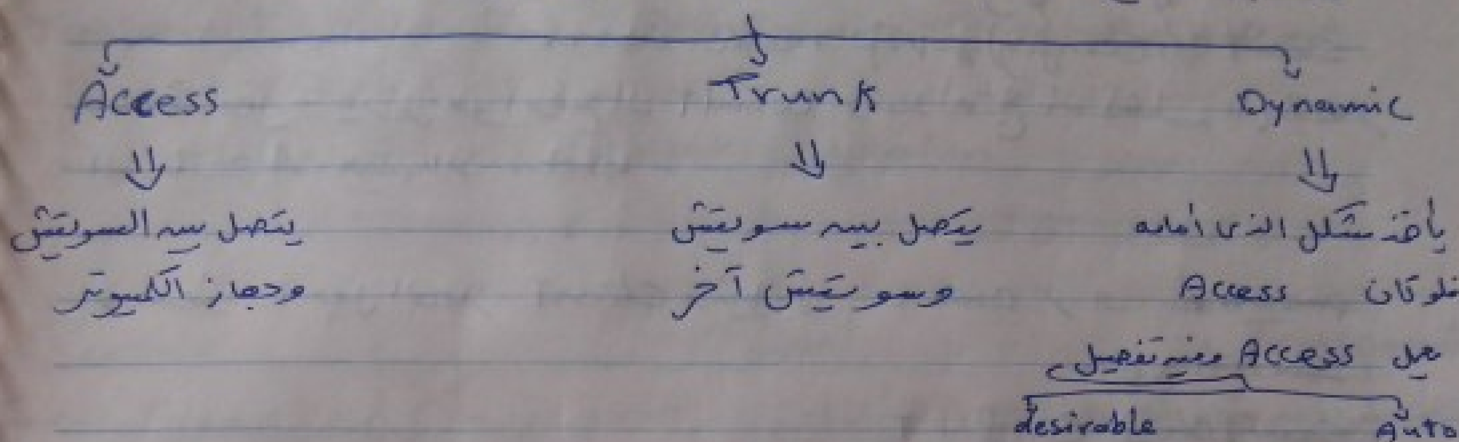
* VTp ← بروتوكول غير آمن حيث يستطيع أي أحد أنه يحصل على إعدادات ال VLAN بمجرد اتصاله بالسويتش عن طريق بورت Trunk وعن طريق كتابة الأوامر التي تجعله سويتش client ولكن نستطيع

DTP — Daynamic Trunking protocol

تفادي هذه المشكلة لابد أنه نعرف ما يسمى بـ

expected Trunking operational mode

ولفهم المصطلح السابقه لابد أنه نفهم أنه البورت تكونه إما



الآن سنرسم جدول نوضح فيه الحالات

يقابل	Access	Daynamic Auto	Trunk	Daynamic Desirable
Access	Access	Access	Dont use	Access
DynamicAuto	Access	Access	Trunk	Trunk
Trunk	Dont use	Trunk	Trunk	Trunk
Daynamicdesirable	Access	Trunk	Trunk	Trunk

شرح آخر للجدول

① بورت Access أمامه بورت Access النتيجه Access

② بورت Trunk أمامه بورت Trunk النتيجة Trunk

③ بورت Trunk أمامة بورت D Auto ⇐ يتحول الأخير Trunk

④ بورت Trunk أمامة D Desirable ⇐ يتحول الأخير لـ Trunk

⑤ بورت Access أمامه Daynamic ⇐ يتحول الأخير لـ Access

تظهر خطورة هذا الجدول في حالة أنه بفرض أنه البورت في السويتش الذي يصل بجهاز كمبيوتر في الشبكة كانه D.Desirable فلو تم

أصلاً الناس بإزالة الجهاز (PC) وجعل مكانه سويتش وكانه البورت في السويتش الجديد أي نوع من أنواع الـ Daynamic أو الـ Trunk فإنه البورت في السويتش الأصلي سيتحول إلى Trunk فالتالي يستطيع الفرد أنه يحصل على تستخدمه الـ VLAN على السويتش الجديد.

وكذلك الحال لو كانه البورت في السويتش الأصلي في الشبكة Daynamic Auto فلو استطاع تغير الجهاز (PC) وجعل مكانه سويتش وجعل البورت في السويتش الجديد Trunk أو Daynamic Desirable فإنه البورت في السويتش الأصلي في الشبكة يتحول إلى Trunk وبالتالي يستطيع أيضاً الحصول على تستخدمه البيانات.

علاج هذه المشكلة

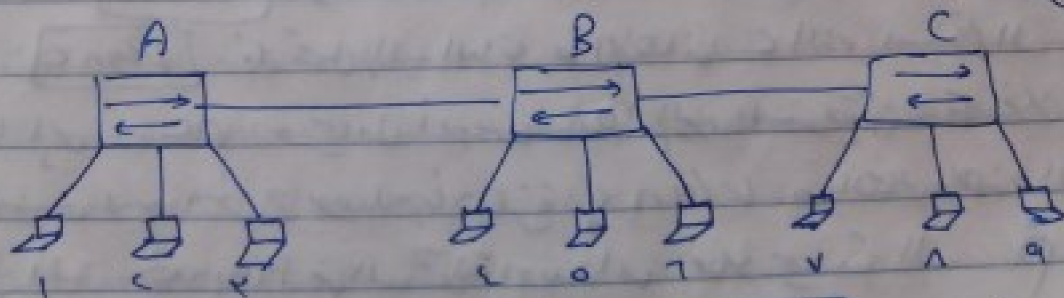
يكمن علاج هذه المشكلة في تعريف البورتات التي تصل إلى أجهزة الشبكة (PCs) على أنها بورتات Access بالتالي لا يستطيع أحد أنه يحصل على بيانات الـ VLAN إلا من طريق سويتشات الشبكة والتي طبعاً يكون لها باسوورد فبالتالي فعلنا الحماية على الـ VLANs ومنع أيضاً عملية التفاوض بين البورتات من طريق الامر switch(config-if) switchport nonegotiate

خصائص بروتوكول VTP

① يقوم بعملية Frame Tagging

يقوم بروتوكول الـ VTP بوضع Tag أو علامة على الـ Frame لكي يفهم السويتش الـ Frame متجهة لأي أجهزة.

مثال

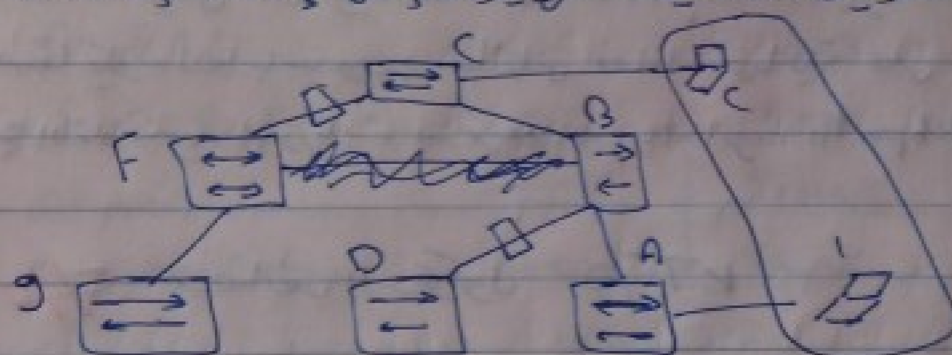


بفرض أنه الأجهزة (1، 4، 8) تبع Vlan 4 لو قام الجهاز رقم ① بإرسال

الـ Frame إلى الجهاز A فإن الـ Frame يخرج من السويتش A ويحصل له Tag أي علامة أنه خاص بالـ Vlan2 فيمر على الجهاز B الذي يعرف أنه أجهزته (1، 3، 4) ليست تبع Vlan2 فبالتالي لا يرسل لأي جهاز منهم الـ Frame ويعلم Tag أنه خرجت من عنده حتى لا تعود إليه مرة أخرى فتخرج حتى تصل إلى الجهاز C الذي يدرك من الـ Tag أنها خاصة بالـ Vlan2 وأنه لديه الجهاز رقم 8 فقط فبالتالي يرسلها إليه فقط ولا يرسلها للآخرين وهذه هي فكرة Frame tagging

② عملية VTP pruning

وهي خاصية تقلل عملية الـ Loop وتقوم فكرتها على أنه إذا كان جهاز يرسل إلى جهاز آخر وكل منهم مرتبط بسويتش مختلف لكنهم تبع Vlan2 مثلاً فإن السويتش الذي له مخرج يوصلني لـ Vlan2 يستقبل الداتا حتى ولو لم تكن الأجهزة الخاصة به مرتبطة بـ Vlan2 وأما السويتش الذي ليس له مخرج يؤدي إلى Vlan2 فإن الداتا لن تصل إليه أصلاً



في هذا المثال الجهاز (PCs 1، 2) تبع Vlan2 عند إرسال PC1 إلى PC2 فإن السويتشات A سيخرج منها الـ Frame يذهب إلى B والجهاز B يرسلها إلى الجهاز C والجهاز D لكن الجهاز C فقط هو الذي لديه مخرج لـ Vlan2 فإنه يستقبل الـ Frame في حين D ليس لديه مخرج يوصله بـ Vlan2 فلا تصل إليه الداتا والجهاز C الذي استلم الـ Frame يسلمها إلى PC2 ويحاول أن يسلمها إلى السويتش F فلا يستلمها F لأنه ليس لديه مخرج يوصله بأجهزة Vlan2 وبالتالي وبهذه الطريقة لا تنتشر الـ Frame في الشبكة دون داعي فلا يحدث الـ Loop

خاصية الـ Native VLAN

هي باختصار خاصية تقوم على حل مشكلة الـ Tag في السويتشات التي لا تقبل الـ Configuration أو في أجهزة الـ Hup



نفرض أن الجهاز ١،٤،٥،٧ تبع أجهزة الـ Accounting وأنا أنشأت vlan خاصة بالـ Accounting وهي Vlan50 وإذا أراد الجهاز ① مثلاً أنه يرسل رسالة لكل الأجهزة في Accounting فإنه بروتوكول 802.1Q يعمل عملية Tag للـ Frame فتصل للجهاز B والذي معرفاً عليه الـ Vlan50 لكن الجهاز C لأنه Hup ولا يقبل الـ Configuration أو هي كانه سويتش لا يقبل الـ Configuration فلا توجد عليه Vlan50 فبالتالي لن تصل إليه الداتا وحل هذه المشكلة تفعل خاصية الـ Native Vlan وهي باختصار أن نلغي عملية الـ Tag وهذا الالغاء يكون عملية ظاهرية يعني أنه عندما أقول أن VLAN50 ليس لها تاج نص أيضاً علامة أو Tag في الباطن أن هذه الـ Vlan50 ليس لها Tag

فعند مرور الداتا إلى الجهاز C سيقرأها أنها ليس لها تاج وبالتالي هي داتا عادية فيستقبلها ويرسلها إلى الأجهزة المرتبطة به وعند مرورها للجهاز B سيقرأ أن لها تاج وهو أنه ليس لها تاج ظاهري فيستقبلها Vlan50 والتي يميزها أنها ليس لها تاج فيمرر الداتا للأجهزة الخاصة بـ Vlan50 المتصلة به

لكي تفعل الـ Native Vlan تذهب لكل سويتش وتعرف الـ Native Vlan

```
switch>en
Switch#Config T
switch(config)# int Fo/1
Switch(config-if)#switchport Trunk native vlan 50
```

فكرة هو البورت الـ Trunk في السويتش

Allowed Vlan

هام

في بعض الأحيان قد نود أنه يسمح البورت الـ Trunk باستقبال البيانات والرسائل الخاصه بـ vlan معينة لكن في احيان أخرى لا نرغب في السماح بـ vlan معينه أيضا في هذه الحالة نستخدم بعض الـ Configuration

```
switch >en
switch # Config t
Switch(config) # int Fo/1
```

نحدد البورت الـ Trunk

الامر الاساسي

```
switch (config-if) #switchport Trunk allowed
```

① في حالة السماح بكل الـ vlans

```
switch(config-if) #switchport Trunk allowed All
```

② في حالة إضافة vlan إلى القائمة المسموح بها

```
switch(config-if) #switchport Trunk allowed vlan add vlan ex
```

10 مثلاً

③ في حالة السماح بكل الـ vlans باستثناء واحدة

```
switch(config-if) #switchport Trunk allowed vlan expet 10
```

مثلاً

④ في حالة إزالة vlans مسموح بها

```
switch(config-if) #Switchport Trunk allowed vlan remove 5-10
```

مثلاً

هام

بعض السويتشات القديمة تعمل بنظام أو البروتوكول ISL مع نظام تعاملهما الـ vlan تستخدم 802.1q أو ISL لكن 802.1q هو الأكثر استخداماً لكن بعض الاحيان بعض السويتشات ISL بصورة تلقائية فعند تعريف البورت على أنه Trunk نحتاج أيضاً أن نعرف البروتوكول الذي سيعمل معه وهو 802.1q

```
switch (config-if) # switchport mode Trunk
switch(config-if) #switchport Trunk encapsulation dot1q
```

تكملة كلام ضمان الأجهزة الحديثة قد لا تحتاج إلى تعريف البروتوكول dot1q عند تعريف الـTrunk

VLAN Full Configuration

1 Vlan Creation:

```
Switch(config)# vlan 100 ex
Switch(config-vlan)# Name Accounting ex
```

2 Access port Configuration

```
switch(config-if)# switchport mode Access
Switch(config-if)# Switchport nonegotiate
Switch(config-if)# switchport Access vlan 100 ex
```

3 Trunkport Configuration

```
switch(config-if)# Switchport mode Trunk
switch(config-if)# switchport Trunk encapsulation dot1q
switch(config-if)# switchport Trunk allowed vlan 10 or 20-30 ex
switch(config-if)# Switchport Trunk native vlan 100 ex
```

4 VTP Configuration

```
switch(config)# VTP mode [server or Client or Transparent]
Switch(config)# VTP Domin <Name>
Switch(config)# VTP password <123 ex>
Switch(config)# VTP pruning
Switch(config)# VTP version [1 or 2]
```

5 Troubleshooting

Switch # show vlan
Switch # show interface [status & switchport]
Switch # show interface Trunk
Switch # show VTP status
Switch # show VTP password

CDP - protocol

هو بروتوكول خاص بأجهزة سيسكو أي أنه يعمل على روترات وسويتشات سيسكو وهو اختصار " Cisco Discovery protocol " يعمل فقط على أجهزة سيسكو أي أنه إذا كان هناك توجيه مختلفة فإنه لا يعمل.

- وظيفته :- هو بروتوكول خاص بالمراقبة والمتابعة عن طريقه نستطيع التعرف على جيران السويتش وهذا البروتوكول مفيد جداً حيث يمكننا من معرفة تصميم الشبكة من خلال معرفة الأجهزة المجاورة لكل جهاز.

* الأوامر الخاصة بـ CDP

1 أمر Show CDP

Switch>en
Switch # show cdp

عند إجراء هذا الأمر ستظهر لنا المعلومات التالية

Global cdp information :
Sending CDP packets every 60 seconds
Sending a hold time value of 180 seconds
Sending CDPv2 advertisements is enabled

Sending cdp packets every 60 seconds

أهل معلومة وهي
الـ cdp packets هي عبارة عن بكت تعريفية ترسل بصورة دورية بين الأجهزة المرتبطة مع بعضها البعض والتي تتضمن المعلومات حول الجهاز المرسل وترسل هذه البيانات كل ٦٠ ثانية

- في حالة توقف احد الأجهزة المجاورة عن العمل أو حدث قطع في الاتصال أو الغاء تفعيل البروتوكول فإنه سيتوقف عن ارسال الـ cdp packets وسوف يحذف من قائمة الأجهزة المجاورة : cdp neighbour بعد ١٨٠ ثانية وهذه المدة هي التي نعرفها بـ : Holdtime :

- الـ Holdtime معناها أن الجهاز : راوتر أو سويتش : سينتظر ١٨٠ ثانية قبل أن يقوم بحذف الجهاز المجاور من القائمة في حال عدم ارساله لـ cdp packets

5 أمر show cdp neighbour

Switch # show cdp neighbour

عند اجراء هذا الأمر ستظهر لنا المعلومات التالية :

Device ID	Local interface	Holdtime	Capability	platform	port ID
switch	Fo/1	180	S	2950	Fo/2
↓	↓	وقت الـ Holdtime	↓	↓	↓ مخرج السويتش الآخر
اسم الجهاز المجاور	مخرج جهازي المتصل بالسويتش المجاور	ويقل تدريجيا إلى أن يصله الـ cdp packet فيرجع لوراء ليصبح إلى ١٨٠ ثانية أو يقل عند عدم الاستلام إلى أن يحذف الجهاز	نوع الجهاز هل هو سويتش R	رقم الموديل	

مثال



في هذا المثال عند اجراء الأمر Switch # show cdp neighbour

على السويتش رقم ٢ ⟸ S2

سيظهر لنا التالي

Device ID	local interface	Holdtime	capability	platform	port ID
S1	Fa0/2	180	S		
↓	↓	↓	↓	2950	Fa0/1
اسم الجهاز المجاور	مخرج الجهاز الذي تنفذ عليه الامر	تقل كل ثانية	سويتش	رقم الموديل	بورت الجهاز المجاور

٣ أمر Show cdp neighbour Detail	① show cdp entry switch

يقوم هذا الامر بإظهار معلومات عن

١ـ IOS ← نظام التشغيل

٢ـ IP address ← للجهاز المجاور

٣ـ نمط الـ duplex للاترسنس في interface المجاورة

٤ أمر منع أو تعطيل البروتوكول وإعادة تشغيله

Switch(Config) # No CDP Run — تعطيله

Switch (config) # CDP Run

• تعطيله وتفعيله على بورت معين ؛

Switch (config) # int Fa0/1 — تحديد البورت

Switch(config-if) # No CDP enable — تعطيله

Switch(config-if) # CDP enable

⑤ أمر تعديل وقت cdp packet و Holdtime

* switch(config) # cdp timer 90

هنا غيرنا وقت ارسال cdp packet من ٦٠ ثانية إلى ٩٠ ثانية

* switch(config) # cdp Holdtime 240

هنا غيرنا ال Holdtime من 180 إلى 240 ثانية

• نستطيع تغيير الوقت كما نريد والقيم في الأوامر السابقة كمثال.

⑥ أمر معرفة كام باكت تم ارساله واستقباله

switch # show cdp Traffic

Etherchannel

ال etherchannel هي تقنية خاصة بسيسكو تسمح بجمع ما يصل إلى ثمانية لينكات حقيقية physical links بين السويتشين تجمعهم في Logical link واحد وهمي



مثال

في هذا المثال يتصل السويتش (S1) بالسويتش (S2) بأربعة لينكات
وكما علمنا فإن بروتوكول STP يقوم بتشغيل لينك واحد فقط واعتبار الباقي كبدائل في حالة التلف ولا يسمح بتشغيل أكثر من لينك لمنع عملية اللوب (Loop)
تكمن ال etherchannel في اعتبار هذه اللينكات الأربعة كأنها لينك واحد والاستفادة منهم على أنهم لينك واحد.

فوائدها

١- زيادة الـ Bandwidth

لو اعتبرنا أن الليتك الواحد هو ١٠٠ ميجا / ثانية فإني استطيع أن أستفيد بـ ٨ أضعاف هذا الرقم حيث أقصى ما يمكن جمعه هو ٨ كابلات في logical link فأستطيع الاستفادة بـ ٨٠٠ ميجا / ثانية

٢- استمرار النقل في حالة انقطاع لينك : Redundancy :

اذا كان لدي في الـ Bundle ٨ لينكات فإذا تلف أحدها فإن الباقي وعددهم سبعة يستطيعون نقل الداتا دون أن تتأثر بالكابل التالف

٣- تقوم بعمل Load Blancing

حيث تقوم بتوزيع الـ Frame على اللينكات بشكل متساوي نسبيًا مما يقلل الضغط على كابل واحد فقط.

شروطها

٥ أن تكون جميع البورتات من نفس الـ vlan أو أن تكون جميعها Trunk أو لكل البورتات Access

① أن يكون كل Bundle بحد أقصى ٨ لينكات وبحد أدنى ٢

② أن يكون بين كل سويتشين 2 Bundle بحد أقصى وبالتأكيد البندل الثانية ستعمل : Redundancy أي أن بروتوكول STP سيوقفها عن العمل إلا في حالة تلف الـ Bundle الأولى.

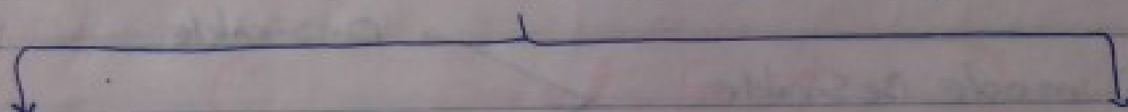
٣- كل البورتات في الـ Bundle لا بد أن تكون من نفس السرعة و Duplex mode

إعداد الـ Etherchannel

يمكن إعداد الـ ether channel بطريقتين
- Manual Bundling يدوية
- Automatic Bundling أوتوماتيكية.

1 Manual Bundling ← الطريقة اليدوية
في هذه الطريقة نحدد البورت الذي نقوم بتنفيذ الأمر عليه
switch (config) # int Fo/1
أو
Switch (config) #int range Fo/1-3
Switch (config-if) # channel-group 1 mode on
ونذهب للسويتش الآخر ونعمل نفس الخطوات ونتأكد من mode on في الجانب الآخر "السويتش الآخر"

2 Automatic Bundling ← الطريقة الأوتوماتيكية
تعتمد هذه الطريقة على نوعين من البروتوكولات



LACP
"قياسي يعمل مع سيسكو وغيرها"

PAgP
"خاص بسيسكو"
"Desirable - Auto"

* لا يوجد فرق في العمل بين البروتوكولين إلا الأجهزة التي يعمل معها كل منهما
* إذا استخدمنا أحد البروتوكولين في سويتش لابد أن نستخدمه في السويتش الآخر

1 PAgP

Switch (config) # int range Fo/1-3
Switch (config-if) # switchport mode Trunk
Switch (config-if) # channel-protocol PAgP حددنا البروتوكول
Switch (config-if-range) # channel-group 1 mode desirable
حددنا المود desirable الخاص ببروتوكول PAgP فلابد أن يقابله "Desirable أو Auto"
Switch (config-if-range) # No Shoutdown
Switch (config-if-range) exit.

LACP ⓒ

```
switch (config) # int range Fa0/1-3
Switch (config-if-range) # switchport mode Trunk
Switch (config-if-range) # channel-protocol LACP
switch (config-if-range) # channel-group 1 mode active
switch (config-if-range) # no shutdown
switch (config-if-range) # exit
```

هذا المود على انه Active فلازم يقابله Active أو passive

* أحوال المود : modes :

أحوال الـ mode حتى تعمل الـ etherchannel بصورة سليمة.

Switch①		Switch②
① mode on	→	mode on
② mode Desirable	→	Desirable / Auto
③ mode Active	→	Active / passive
④ mode Auto	→	mode Desirable

* أوامر الـ show الخاصة بـ ether channel ، ونستطيع استخدمها.

```
switch # show etherchannel
Switch # show etherchannel port-channel
Switch # show etherchannel Summary
Switch # show ip interface brief
```

الفرق بين الطريقة الـ Manual وطريقة البروتوكولات

الفرق بين الطريقة الـ Manual وطريقة البروتوكولات هي أن طريقة الـ Manual إذا جعلنا عدد من الـلينكات في سويتش في etherchannel فلا بد أن يقابلها في السويتش الآخر etherchannel تضم اللينكات في السويتش الآخر وإلا فإنه تعمل الـ etherchannel بالإضافة إلى تعطل العمل باللينكات منفردة.

طريقة البروتوكولات ← إذا فعلنا etherchannel في سويتش فعلينا تفعيل etherchannel في السويتش الآخر حتى نستفيد منه فكرة عمل الـ etherchannel لكن إذا فعلنا في طرف وطرف آخر لم نفعلها تعمل اللينكات لأنه لم يوجد etherchannel وبالتالي يمكن الاستفادة في نقل البيانات.

port-fast

ذكرنا سابقاً أن البورتات حين تنتقل من وضع Down إلى وضع UP في بروتوكول STP فإنها تستغرق ٥٠ ثانية تقريباً لأنها تمر بمراحل ① Blocking ← ٢٠ ثانية ② Listening ← ١٥ ثانية ③ Learning ← ١٥ ثانية

فلكي يتم تنفيذ "Rapid-pvst" أي نتجاوز فترة الـ ٥٠ ثانية لابد أن نفعل خاصية الـ port Fast على البورتات المتصلة بأجهزة الكمبيوتر "Access" ولتفعيلها نتبع الآتي.

تحديد البورت
```
Switch(config)# int Fo/1
```
تفعيل الأمر
```
Switch(config-if)# spanning-Tree portfast
```

بعدها نستطيع تنفيذ أمر rapid pvst

```
switch(config)# spanning-Tree mode rapid-pvst.
```

Switch Remote management

وضحنا سابقا أن طريقة الدخول على إعدادات السويتش تكون عن طريق كابل الـ Console وباستخدام برنامج Hayper term أو برنامج TeraTerm للدخول على السويتش وبدء عملية الـ Configuration

* هناك طريقة أخرى هي طريقة الدخول عن بعد أي عن طريق جهاز من أجهزة الشبكة يمكنه الدخول على اعدادات السويتش وكذلك بشروط نبدأ الآن في توضيحها.

* يمكن أن يتم التحكم في السويتش عن بعد اما عن طريق ssh أو عن طريق الـ Telnet.

اعدادات الـ Remote Access

1. اعداد Ip للسويتش
2. تفعيل الـ Remote Access ووضع باسوورد
3. عمل password على privileged mode
4. اعداد Ip للراوتر " Get way "

1 إعداد الـ Ip للسويتش

* في البداية السويتش لا يتعامل بـ Ip لكن الشئ الوحيد الذي استطيع أن أضع عليه Ip هو الـ Vlan
* الجهاز الذي يستطيع الدخول عن بعد هو الجهاز المشترك مع الـ Vlan الذي نعطيه Ip ويكون له نفس العنوان للشبكة " Subnet mask "

أوامر السويتش لاعداد Ip

Switch > en
Switch # Config T
Switch # int vlan1 — تحديد الـ interface الخاص بـ vlan1
Switch(Config-iF) # No shut down — تفعيلها أو تشغيل الانترفيس
Switch(Config-iF) # Ip address 192.10.10.1 255.255.255.0
Switch(Config-iF) # exit — اعطاء الـ IP وكتابة الـ السابنت ماسك

٢ تفعيل الـ Remote access

لو عملنا أمر Show Run على السويتش هيظهر لنا

Line Con 0 ⟵ الـ Console

Line vTy 0 4 ⟵ معناها أن هناك 5 أجهزة تستطيع الدخول والتحكم عن بعد في السويتش

أوامر السويتش

Switch > en
Switch # Config T
Switch(config) # Line vTy 0 4 — تحديد الانترفيس الوهمي الخاص بأجهزة التحكم عن بعد
Switch (config-line) # password 123 — تحديد الباسوورد لتفعيل التحكم عن بعد
Switch (config-line) # login — السماح لمن يريد عمل login عن بعد
Switch (config-line) # exit

٣ عمل password على الـ privileged mode

Switch (config) # enable secret 123 — مشفرة
switch (config) # enable password 123 — غير مشفرة

لابد من عمل هذه الخطوة وبدونها لا تستطيع الدخول من بعد فهي خطوة مهمة.

بالخطوات الثلاثة السابقة أنهينا إعداد الـ Remote Access بالنسبة للسويتش وبقي أن نستخدم طريقة الدخول Telnet أو SSH

① طريقة الـ Telnet

نذهب إلى الجهاز " PC " الذي نريد من خلاله الدخول والتحكم في السويتش عن بعد

١- ندخل قائمة start ونختار Run ثم نكتب الأمر cmd

٢- بعد الدخول لوضع cmd نكتب الأمر Telnet كالتالي

Telnet 192.10.10.1

أي أننا نكتب Telnet ثم نكتب الـ IP الخاص بالسويتش الذي وضعناه للـ Vlan بعدها نستطيع الدخول والتحكم في السويتش بعد كتابة الـ password

(هام) طريقة الـ Telnet طريقة غير آمنة حيث يتم إرسال البيانات دون تشفير فيستطيع أحد الهاكرز باستخدام برامج Sniffing أن يتعقب الداتا الخاصة بـ IP معين وبالتالي يمكنه الحصول على الـ password وبالتالي التحكم في السويتش.

* يستخدم الـ Telnet البورت رقم ٢٣.

② طريقة الـ SSH

هي طريقة أخرى للاتصال عن بعد بالسويتش لكنها أكثر أمانا من طريقة الـ Telnet حيث تعتمد على عملية التشفير والـ SSH هي اختصار " Secure Shell "

ويستخدم هذا البروتوكول البورت ٢٢

* شروط استعمال

١- لابد من تغيير الاسم الـ Default للسويتش

٢- إنشاء username و password

٣- إنشاء Domainname يكون بمثابة عنوان لكل الأجهزة التي تدخل عن بعد

أوامر تفعيل الـ SSH

switch > en
Switch # Config T

① تغير اسم السويتش
Switch(config)# Host Ahmed (or) hostname Ahmed

② إنشاء username و password
Switch(config)# Username Tarek secret 1234

③ إنشاء Domin name
Switch(config)# Ip Domin-name egypt.com
ويكون الـ Domin ينتهي بـ com. أو org. أو net.

④ تفعيل التشفير ــ لابد من تغير اسم السويتش كما سبق
~~Switch~~ Ahmed(config)# Crypto Key generate rsa

هكذا نكون انتهينا من الاعدادات الخاصة بـ SSH والاعدادات تكون مشفرة.

⑤ تحديد الداخل عن طريق Remoteaccess واجبارة على استخدام SSH
Ahmed(config)# Line vTy 0 4 — الأجهزة المسموح للدخول بـ Remote
Ahmed(config-Line)# Transport input SSH — استخدام SSH فقط
Ahmed(config-Line)# login local

الأمر الأخير لمنع الدخول للسويتش باستخدام SSH إلا عن طريق الـ LAN الداخلية المتصلة فعلاً بالسويتش وعدم السماح لأي أحد خارج الـ LAN بالدخول مثل من يدخل من البيت عن طريق النت

طريقة الدخول

١- نذهب لـ start في الجهاز الذي سنشغل منه عليه السويتش

٢- نختار Run أو نختار cmd

٣- بعد الدخول لـ cmd نكتب :

SSH -L username Ip switch

أي ستكون الصورة

SSH -L Tarek 192.10.10.1

بعدها سيطلب الباسورد

password : 1234

وبعدها نكتب الباسورد الخاصة بالـ privileged ونتابع العمل

هام: هذه الطريقة خاصة ببرنامج المحاكاة "Packet Tracer"

لكن في الحقيقة نستخدم برنامج putty

١- نختار الاتصال SSH

٢- نكتب Ip الخاص بالسويتش

٣- نختار open

بعدها سيفتح النافذة التي نستطيع كتابة الأوامر عليها

أوامر الـ SSH كاملة

```
Switch(config)# host S1
S1(config)# username Ahmed secret 1234
S1(config)# Ip Domin-name egypt.com
S1(config)# Line vTy 0 4
S1(config-line)# Transport input SSH
S1(config-line)# login local
S1(config-line)# exit
```

عملية حفظ الـ Configuration

نحتاج بعد عمليه ضبط الـ Configuration أن ننقل هذه الـ Configuration من الـ RAm إلى NVRAm لأننا لو تركناها على الـ RAm فإنه عند انقطاع التيار الكهربي مثلا سيبدأ السويتش العمل من عودة التيار الكهربي ولم يتم حفظ الـ Configuration وبالتالي لن تكون موجودة.

switch # copy Run start — لحفظ الـ config في NVRam

(Run) تمثل RAm — (start) تمثل NVRam

(RAm) هي ذاكرة يتم تخزين الاوامر عليها ولكنها تفقد كل بياناتها عند انقطاع التيار الكهربائي أو عند اعادة التشغيل للجهاز لذلك نحتاج إلى ذاكرة تخزين دائمة مثل NVRam

(NVRam) هي ذاكرة يتم تخزين أوامر بدء التشغيل عليها "startup-config" وهي اختصار "nonvolatile Ram" أي ذاكرة غير متطايرة وتجعل أوامر السويتش دائمة فيتم نقلها من الـ Ram إلى NVRam

(Flash memory) هي ذاكرة يتم بها حفظ نظام التشغيل الخاص بالسويتش أو الراوتر لا تفقد بياناتها عند انقطاع التيار لكنه هي قابله لاعادة التهيئة وتحميلها بنظام تشغيل آخر بدلا من استبدالها لذلك هي تشبه تكون الفلاشة الموجودة حاليا.

أوامر الـ copy.

switch # Copy Run start

وهو حفظ الـ config في الـ NVRam

switch # erase start

وهو أمر ازالة الـ config من NVRam

مصطلحات هامة

1 BroadCast

هو عملية ارسال الداتا إلى جميع الـ Hosts الموجودة على الشبكة
ويجب معرفة أنه لكل شبكة network address و BroadCastaddress خاص بـ

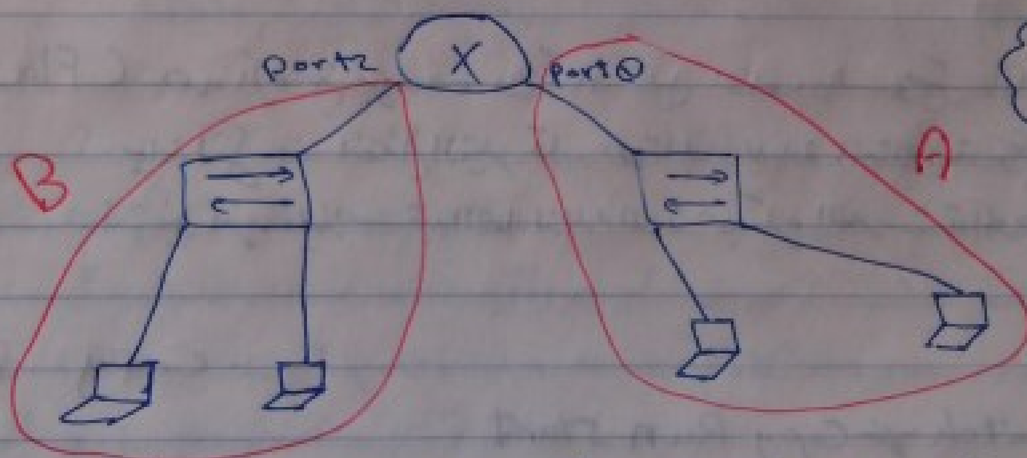
مثال

إذا كان لدينا شبكة عنوان 10.0.0.0/8 فإن الـ BroadCast لهذه الشبكة هو 10.255.255.255 أي أن BroadCast address هو عنوان الـ Ip الأخير في الشبكة الذي يتم عن طريقه ارسال البيانات إلى جميع الـ Hosts

2 BroadCast domain

كما ذكرنا فإن عملية الـ BroadCasting تحدث داخل الشبكة الواحدة لذلك فإن نطاق البرودكاست " BroadCast domain " هو عند حدود نطاق هذه الشبكة

مثال



في هذا الشكل لدينا شبكتين كل شبكة عبارة عن السويتش وأجهزة الـ PC متصلة بپورت في الراوتر

A الشكل A هو الـ BroadCast domain لهذه الشبكة

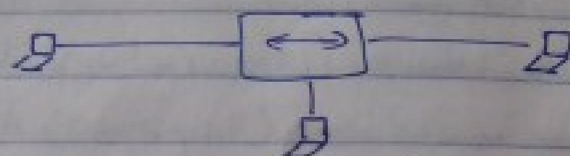
B الشكل B هو الـ BroadCast Domain لهذه الشبكة

Collision domain [٣]

الـ Collision domain أو نطاقات التصادم هو مصطلح لفهمه لابد أن نفهم أولاً ما هو الـ Collision أو التصادم.

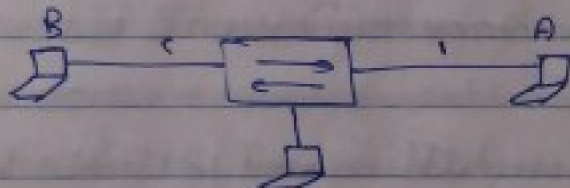
الـ Collision ⇐ يحدث عندما يقوم جهازين أو أكثر بإرسال داتا في نفس الوقت.

(مثال)



في هذا المثال لدينا جهاز Hup وثلاثة أجهزة pcs والـ Hup من أجهزة Layer① وهو لا يستطيع التعرف على IP أو الـ mac address لذلك فإنه يرسل الداتا لكل الأجهزة المتصلة به كـ Broadcast "أي لجميع الأجهزة" ويستقبلها الجهاز التي أرسلت إليه في الأصل والباقي لا. فماذا يحدث إذا أرسل جهازين أو أكثر في نفس الوقت مع العلم أن الـ Hup ذو خاصية الـ Half D. أي أنه إما يرسل وإما يستقبل ليس الاثنان معاً. في هذه الحالة سيحدث عملية تصادم للداتا "Collision" في جميع تفرعات الـ Hup

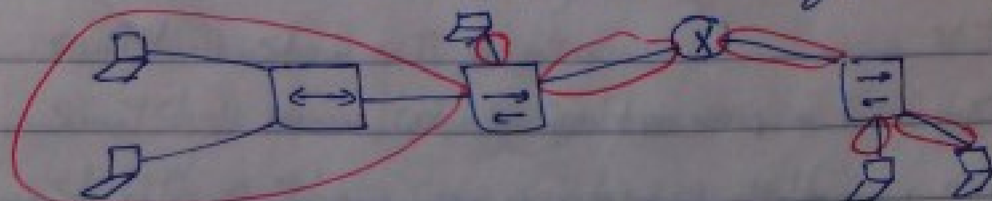
(مثال ٢) المثال السابق نستبدل الـ Hup بسويتش



السويتش من أجهزة Layer2 أي أنه يميز الـ macaddress وبالتالي يمكنه توجيه البيانات تجاه الجهاز الصحيح مباشرة بعد إرسالها لباقي الأجهزة وهذا يعني أن التصادم لن يحدث في كل تفرعات السويتش بل في مسار واحد فقط وهو إذا أراد الجهاز A مثلاً إرسال داتا لـ B وكان B يرسل أيضاً لـ A فهنا يحدث تصادم إما في الكابل الأول أو الثاني حسب مكان تصادم الداتا. نستخلص من ذلك الآن

Collision Domain ⇐ هو الحد الذي ينتهي عنده حدوث الـ Collision

(مثال)



كل تفريعات السويتش اعتبرت كل واحدة Coll D. في الـ وكذلك اللينك بين الراوتر والسويتش

الـ Hup اعتبر هو وتفريعاته كاملة Collision D. لأنه يرسل الداتا Broadcast فاحتمال التصادم أكبر

ملخص هام لأوامر السويتش

1 Switch Modes

Command		Mode
Switch > enable	→	user mode
Switch #	→	privileged mode
Switch(config)#	→	Global mode
Switch (config-if) #	→	Interface mode
Switch (config-subif) #	→	Subinterface mode
Switch(config-line) #	→	Line mode

2 Help Commands

Command	Description
Switch > ?	show List help Command

3 Show Commands

Command	Description
Switch # show version	software & hardware info
Switch # show Flash	Flash memory info
Switch # show mac-address-table	
Switch # show Running-config	Config. in Ram
Switch # show Startup-config	Config - in nvRam
Switch # show vlan	vlan Configuration
Switch # show Interfaces	Interface information
Switch # show spanning-Tree	STP. information
Switch # show VTP status	VTP. info.
Switch # show cdp neighbors	list of CDP neighbors
Switch # show cdp neighbors details	more info about neighbors

Switch # show ip interface brief — معلومات البورت والـ IP البورت

Switch # show etherchannel

4 Reset Switch Config.

① Switch # delete Flash : vlan.dat

  Delete Filename [vlan.dat]? (enter) ← press

  Delete Flash vlan.dat? Confirm (enter)

② Switch # erase startup-config

③ Switch # Reload

5 To Set hostname

Switch # config T

Switch (config) # hostname S1 or host S1

S1 (config) # exit

6 To Set password

A- privilegedmode

switch (config) # enable password ex — غير مشفرة

switch (config) # enable secret ex — مشفرة

switch (config) # Service password-encryption — تشفير الغير مشفرة

B- Console mode

switch (config) # line Console 0

switch (config-line) # password ex

switch (config-line) # login

switch (config-line) # exit

C - VTy mode

Switch(config) # line vTy 0 4
Switch(config-line) # password ex
Switch(config-line) # login
Switch(config-line) # exit

7 Speed and Duplex

Switch(config) # int Fo/ex
Switch(config-if) # duplex half or Full or Auto
Switch(config-if) # speed 10 or 100 or Auto

8 port Security

Switch(config) # int Fo/ex
Switch(config-if) # switchport mode Access
Switch(config-if) # switchport port-security
Switch(config-if) # switchport port-security mac-address ex
or Switch(Config-if) # Switchport port-security mac-address sticky
Switch(config-if) # Switchport port-security maximum ?...
Switch(Config-if) # Switchport port-security mac-address ex
Switch(config-if) # switchport port-security voilation shutdown or protect
restrict
Switch(config-if) # exit
Switch(config) # exit
Switch # Show port-security address

9 STP

① تحديد جهاز على انه الروت

```
Switch(config)# spanning-Tree vlan 1 Root primary
```

② خاصية الـ Rapid-pvst

• اولاً تفعيل البورت فاست

```
switch(config)# int Fo/ex__
switch(config-iF)# spanning-Tree portFast
```

• تفعيل الـ Rapidpvst وتكون على كل السويتشات

```
Switch(config)# spanning-Tree mode Rapid-pvst
```

```
switch # show spanning-Tree
```

10 VLAN

• Creation vlan

```
switch(config)# vlan_ex
Switch(config-vlan)# Name_ex__
```

2- Access port Config.

```
switch(config-iF)# switchport mode Access
Switch(config-iF)# Switchport nonegotiate
Switch(config-iF)# switchport Access vlan_ex
```

3- Trunk ports Config.

```
Switch(config-iF)# switchport mode Trunk
Switch(config-iF)# Switchport Trunk encapsulation dot1a
Switch(config-iF)# Switchport Trunk allowed vlan_ex
Switch(config-iF)# Switchport Trunk native vlan_ex
```

11 vTp

Switch (config) # vTp mode [server - client - transparent]

Switch (config) # vTp Domain _ ex _

Switch (config) # vTp password _ ex _

Switch (config) # vTp pruning

Switch (config) # vTp version

Switch # show vTp status

Switch # vTp password

12 CDP

Switch # show cdp neighbors

Switch # show cdp neighbors details

Switch (config) # CDP Run — تفعيل

Switch (config) # No cdp Run — تعطيل

Switch (config-if) # CDP enable — تفعيل لبورت

Switch (config-if) # No cdp enable — تعطيل لبورت

Switch (config) # Cdp timer _ ex _ — تعديل وقت cdppacket

Switch (config) # Cdp Hold time _ ex _ — تعديل الHoldtime

Switch # show cdp Traffic — معرفة كم باكت تم ارساله واستقباله

13 EtherChannel

① manual

Switch (config) # int Fo/ _ ex _

Switch (config-if) # channel-group 1 mode on

وتفعل الأمر على السويتش الآخر

② Automatic

```
Switch(config)# int Fo/_ex
Switch(config-if)# Switchport mode Trunk        تحويل البورت لـ Trunk
Switch(config-if)# channel-protocol _PAgp_      بروتوكول PAgp
or  switch(config-if)# channel-protocol _lAcp_  بروتوكول lAcp
Switch(config-if)# channel-group 1 mode _desirable_   (PAgp)
or  Switch(config-if)# channel-group 1 mode _Active_  (LAcp)
Switch(config-if)# No Shutdown
Switch(config-if)# exit
Switch# show etherchannel
Switch# Show etherchannel Summary
Switch# show etherchannel port-channel
```

19 Remote Access

① اعداد Ip السويتش

```
switch(config)# int vlan 1
Switch(config-if)# No shutdown
Switch(config-if)# Ip address _ex 10.1.1.0_   _255.0.0.0_
Switch(config-if)# exit
```

② تفعيل الـ Line vTy password

```
switch(config)# line vTy 0 4
Switch(config-line)# password _ex_
Switch(config-line)# login
Switch(config-line)# exit
```

③ تفعيل privileged password

```
Switch(config)# enable password _ex_
or  Switch(config)# enable Secret _ex_
```

15 SSH

Switch(config) # host S1 — تغير اسم السويتش

Switch (config) # username ex Secret ex — انشاء اليوزر والباسورد

Switch(config) # Ip Domain-name ex.com

S1 (config) # Crypto key generate rsa — تفعيل التشفير ولابد تغير اسم السويتش

• تحديد الداخل بـ SSH فقط

S1(config) # line vTy 0 4

S1 (config-line) # Transport input SSH

S1 (config-line) # login local — منع الدخول الا من LAN

S1 (config-line) # exit

IP Subneting

* تعريف الـ Ip address

هو عنوان رقمي يتم تعيينه لكل جهاز على الشبكة بحيث يصبح عنوان خاص بالجهاز للإشتراك مع جهاز آخر على الشبكة يسهل هذا العنوان الوصول للجهاز ويسمح له بالاتصال بغيره من الأجهزة.

* شكل الـ Ip

يتكون الـ Ip ٤ خانات تسمى octet يفصل بين كل octet وآخر علامة عشرية [dot] كما يظهر بالمثال 192.168.1.15 Ip

كل octet مكون من 8Bit ٨ بت والـ Bit عبارة عن رقم وله قيمه واحد أو صفر أي أن الـ octet مكون من ٨ وحايد أو ٨ اصفار أو ٨ وحايد وأصفار

بالتالي الـ Ip = 32Bit حيث أنه = ٤ octet والـ octet = ٨Bit

∴ Ip = ٤ octet X ٨ Bit = 32Bit

Ip = 32Bit

* يتم كتابة الـ Ip بإحدى الطرق الآتية

١- باستخدام النظام العشري "Delimal" مثال ١٠.١.١.٢

٢- باستخدام النظام الثنائي "Binary" مثال

11111111.11110000.10011010.00111110

وهو ثنائي لأنه لا يستخدم إلا الواحد والصفر

3- باستخدام النظام السداسي عشري "hexadecimal" مثال

"AC 10 IE 38"

هذا النظام الأخير يستخدم في سجل النظام Windows Registry

وبالطبع أكثرهم استخداماً هو باستخدام النظام العشري مثل ١٠.١.١.٢

* عنوان الشبكة Network address
هو عنوان يستخدم لإرسال البيانات إلى شبكة محددة عديدة ومن الأمثلة
عليه 10.0.0.0 أو 172.16.0.0 أو 192.168.10.0

• Broadcast address
هو العنوان الذي يستخدم من قبل الأجهزة والتطبيقات لإرسال المعلومات لجميع الأجهزة
على الشبكة ومن الأمثلة عليه: 10.255.255.255 والذي يقوم بإرسال البيانات لجميع أجهزة
الشبكة 10.0.0.0 مثال آخر 172.16.255.255 هو ال BroadCast للشبكة
172.16.0.0 وكذلك 192.168.10.255 هو ال BroadCast للعنوان 192.168.10.0

* هذان العنوانان ال Network address و BroadCast لا يتحصل عليهما أي جهاز في
الشبكة لكن ما بينهما هي العناوين المتاحة لأجهزة الشبكة وكل جهاز يسمى
Host ويكون له عنوان غير الآخر ولكن كلاهما مشتركين في نفس الشبكة
(مثال) الجهاز A له Ip = 10.21.21.1 والجهاز الثاني له 10.21.21.2
فهذا له عنوان و الآخر له عنوان
(مثال آخر) جهاز له Ip 192.168.1.2 والآخر 192.168.1.3 نلاحظ
أنها يشتركان في نفس عنوان الشبكة وهو (192.168.1) لكن اختلاف في
عنوان كل منهما في الأول 2 والثاني 3

مفهوم ال Subnetmask
هو رقم يتكون أيضاً من ٣٢ Bit مقسمة أيضاً إلى ٤ octet يكون هذا الرقم مرافقاً
لل Ip و Subnetmask بعض معلومات حول الشبكة التي ينتمي إليها ال IP address
من حيث معرفة عنوان الشبكة سواء كانت رئيسية أو فرعية ومن حيث معرفة عدد الهوست
الممكنة في هذه الشبكة.

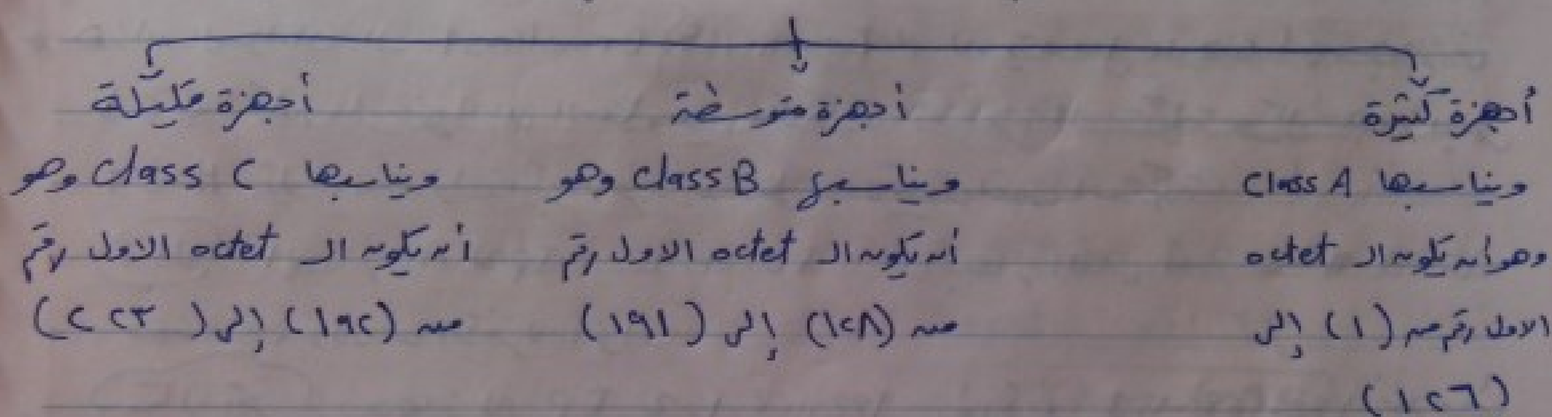
أي شبكة أهم ما يجب مراعاة كتابته بصورة سليمة هو ال Ip address
وال Subnetmask

• عند كتابة Ip على جهاز كمبيوتر يقوم نظام التشغيل بكتابة ال Subnetmask بصورة تلقائية

أي Ip كما ذكرنا يتكون من ٤ octet وكل octet يتكون من رقم من 0 حتى 255 عند كتابة Ip نختار لكل octet رقم من 0 إلى 255 وهذه صورة عامة تكلم فيه بعض التفصيل.

لكن اذا كتبنا Ip عشوائي لكل جهاز من أجهزة الشبكة قد يؤدي ذلك إلى الخطأ وعدم القدرة على متابعة الشبكة ومعرفة أماكن الأجهزة في الشبكة في شركة ما مثلاً لذلك قامت منظمة شهيرة بإيجاد حل لمشكلة العشوائية هذه وتلك المنظمة هي منظمة IANA [Internet Assigned Number Authority]

قامت هذه المنظمة بتقسيم الشبكات حسب الحجم إلى ثلاث أنواع



• بالاضافة إلى class D من (٢٢٤) إلى (٢٣٩)
class E من (٢٤٠) إلى (٢٥٤)

رقم 127 لم يتم ادراجه لأنه مخصص لعملية ال Troubleshooting

فيكون الشكل النهائي لجميع ال classes مع ال Subnetmask

class	Range	Default mask	Hosts
A	1 - 126	255.0.0.0	١٦,٧٧٧,٢١٤
B	128 - 191	255.255.0.0	٦٥,٥٣٤
C	192 - 223	255.255.255.0	٢٥٤

للفهم فقط

وللفهم كيف تم تحديد هذه الأرقام لابد أن ندرك أن الذي يحدد ال class هو ال octet الأول.

① في ال class A

قامت IANA باعتبار أن ال class الأول في هذا ال octet عند تحويله للنظام الثنائي أن يبدأ أول Bit فيه بالرقم صفر فكان أول رقم ظهر هو 00000001 وهو ما يقابله بالعشري الرقم 1 وآخر رقم قد يظهر باعتبار وجوب أن يكون أول Bit = صفر هو رقم 01111111 الذي يقابل الرقم 127 لكن تم حجز هذا الرقم لعملية أخرى فأصبح ال class A هو 1-126

② في ال class B

اعتبرت IANA أن أول Bit = 1 ، ثاني Bit = صفر في ال octet الأول فكان أول رقم 10000000 وهو ما يقابله في النظام العشري 128 وكان آخر رقم هو 10111111 وهو ما يقابله الرقم 191 فكان class B (128-191)

③ في ال class C

اعتبرت IANA أن ال Bit رقم 1 ورقم 2 هو 1 وال Bit الثالث 0 فكان أول رقم 11000000 وهو ما يقابله في النظام العشري 192 وكان آخر رقم هو 11011111 وهو ما يقابله في النظام العشري رقم 223 فكان class C (192-223)

وبذلك تكون فهمنا أرقام كل class

---

* وضح لنا من كل class عدد الأجهزة "Host" في كل class 16 مليون في A ، 65 ألف في B ، 254 في C فنفترض أن لدي شبكة مكونة من 100 جهاز وإذا اخترت class A نجد أنه يحوي عدد أجهزة ما يزيد عن 16 مليون جهاز فعند إرسال الداتا ☁ كبرودكاست فإن السويتش أو ال Hup يفهم من العنوان أن هناك ما يزيد عن 16 مليون جهاز رغم أنهم حقيقة 100 فقط تكمن في اختيار class غير مناسب تعرفنا عليه أنه 16 مليون فيبدأ في عمل 16 مليون نسخة من البيانات وبالتالي 100 جهاز هم من يستلمون البيانات

والباقي وهو تقريباً ١٦ مليون نسخة ستنقل من الكابلات ما يسبب حدوث Loop وضغط الشبكة وذلك نتيجة اختيار الـ class غير المناسب

مثال آخر: لدي ٥٠٠ جهاز لعمل شبكة بالطبع لا أستطيع أن أختار الـ class صاحب الـ ٢٥٤ جهاز لأنه class أقل من عدد الأجهزة المراد تكوينها لشبكة

بل بالتالي ننتقل إلى الـ class التالي وهو الأكثر منه في عدد الأجهزة وهو الـ class صاحب ٦٥ ألف جهاز تقريباً نجد أنه قابل لتكوين الشبكة صاحبة الـ ٥٠٠ جهاز لكنه سيتم تحويل أكثر من ٦٥ ألف وليس ٥٠٠ جهاز وبالتالي تحدث عملية اللوب وضعف الشبكة.

ولحل هذه المشكلة نستخدم ما يسمى بـ الـ Subneting

Subneting

باختصار الـ Subneting هو عملية تقسيم للشبكة إلى شبكات أصغر

فوائده كثيرة منها:

1. تحسين أداء الشبكة
2. تسهيل إدارة الشبكة
3. تحديد المشكلة بسهولة.

ولفهم عملية الـ Subneting بصورة سليمة لابد أن نفهم عملية التحويل من عشري إلى ثنائي from Decimal to Binary والعكس from Binary to Decimal وهكذا

التحويل بين العشري والثنائي

وضحنا سابقاً أن الـ IP قد يكتب بالصورة العشرية مثل

192.168.10.1

أو بالصورة الثنائية التي تعتمد على رقمين فقط وهما الواحد والصفر مثل

هذا الرقم ١٠١٠٠١١١ . ٠٠٠١٠٠٠١ . ٠١٠١٠٠١١ . ١١١١١١١ كمثال هو رقم ثنائي يعتمد على الواحد والصفر وكل octet يساوي رقم عشري تكلمه كيف يتم التحويل بين الثنائي والعشري.

يتم التحويل بين الثنائي والعشري اعتماداً على أرقام ثابتة يتم استخدامها في عملية التحويل سواء من العشري إلى الثنائي أو من الثنائي إلى العشري هذه الارقام هي

١٢٨	٦٤	٣٢	١٦	٨	٤	٢	١

١ التحويل من عشري إلى ثنائي

يتم التحويل من عشري إلى ثنائي عن طريق عرض الرقم العشري للطرح بمعنى أدق نقوم بطرح الارقام السابقة من الرقم العشري فإن تقبل الطرح دون نتائج سالبه نضع تحت خانة الرقم ١ وإذا لم يقبل الطرح نضع مكانه صفر والطرح يبدأ من الرقم ١٢٨ وينتهي بـ ١

مثال

كيفية تحويل الرقم ١٩٢ إلى رقم ثنائي.

١٢٨	٦٤	٣٢	١٦	٨	٤	٢	١

نقوم بطرح الرقم ١٩٢ فنقوم بطرح ١٩٢ - ١٢٨ نجد أنه تقبل الطرح والناتج هو ٦٤ ∴ نضع ١ مقابل الـ ١٢٨ أي مكانه الـ Bit الأول من الـ octet الأول

بمعنى أنه ١٩٢ هي الـ octet الاول من IP معين فتكون الصورة ???????1

أي وضعنا ١ في الـ Bit الأول وباقي الـ Bits مازلنا لا نعرفها.

نعود لعملية الطرح نجد الناتج من عملية الطرح الأولى هو ٦٤ نقوم بطرحها من الـ ٦٤ ∴ ٦٤ - ٦٤ ∴ يقبل الطرح فنضع واحد في الـ Bit الثاني والباقي صفر ونقوم بطرح باقي الأرقام | ١ | ٢ | ٤ | ٨ | ١٦ | ٣٢ | من صفر نجد أنه لا تقبل الطرح ∴ نضع مكانه كل Bit صفر

فيكون الرقم الثنائي المقابل لـ ١٩٢ هو **11000000**

مثال آخر

ماهو نتيجة تحويل الرقم ١٢٥ إلى رقم ثنائي.

أولاً نقوم بطرح الأرقام الثابتة ١ ٢ ٤ ٨ ١٦ ٣٢ ٦٤ ١٢٨

من الرقم ١٢٥ فإذا قبل الطرح نضع واحد وإذا لم يقبل نضع صفر وطبعاً الطرح يبدأ من الرقم ١٢٨

١٢٨	٦٤	٣٢	١٦	٨	٤	٢	١
١٢٥ لا يقبل الطرح نضع صفر	١٢٥ يقبل نضع واحد	٦١ يقبل نضع واحد	٢٩ يقبل	١٣ يقبل	٥ يقبل	١ لا يقبل	١
0	1	1	1	1	1	0	1

نلاحظ أنه بعد عملية الطرح نضع واحد إذا قبل الرقم عملية الطرح وندخل بالنتيجة إذا وجد ونطرح من الرقم التالي . فالحالة إذا لم يقبل الطرح نضع مكانه الصفر

فيكون ناتج تحويل الرقم ١٢٥ من عشري إلى ثنائي **01111101**

مثال آخر: حول الـ IP التالي إلى ثنائي بدل عشري :

192.168.1.50

أولاً

نقوم بطرح رقم كل octet ونطرح من الأرقام الثابتة من ١ إلى ١٢٨

octet 1: 192

البت	الرقم الثابت	الباقي
1	١٢٨	192
1	٦٤	٦٤ الباقي
0	٣٢	0 الباقي
0	١٦	0
0	٨	0
0	٤	0
0	٢	0
0	١	0

octet 2: 168

البت	الرقم الثابت	الباقي
1	١٢٨	168
0	٦٤	٤٠ الباقي
1	٣٢	٤٠
0	١٦	٨ الباقي
1	٨	٨
0	٤	0 الباقي
0	٢	0
0	١	0

octet 3

البت	الرقم الثابت	الباقي
0	١٢٨	1
0	٦٤	1
0	٣٢	1
0	١٦	1
0	٨	1
0	٤	1
0	٢	1
1	١	1

octet 4

البت	الرقم الثابت	الباقي
0	١٢٨	٥٠
0	٦٤	٥٠
1	٣٢	٥٠
1	١٦	١٨
0	٨	٢
0	٤	٢
1	٢	٢
0	١	0

11000000	10101000	00000001	00110010

بعد أن قمنا بطرح رقم كل octet من IP أي قمنا بطرح الأرقام الثابتة منه ووضعنا
1 إذا قبل الطرح واحد وإذا لم يقبل صفر نجد أن ناتج تحويل الـ IP ← 192.168.1.50
إلى رقم ثنائي هو:

11000000.10101000.00000001.00110010

٢ التحويل من ثنائي إلى عشري.

في هذه الطريقة يتم أيضاً الاعتماد على نفس الأرقام الثابتة ١ ٢ ٤ ٨ ١٦ ٣٢ ٦٤ ١٢٨
ونعتبر أن الـ octet المكون من 8 Bit هو هذه الأرقام ونذهب للرقم الثنائي
ونضعه تحت هذه الأرقام وما تحته واحد نقوم بجمعه ونتجاهل ما تحته صفر

مثال

حول الرقم الثنائي 11110000 إلى رقم عشري.

الحل

نضع الأرقام الثابتة ونضع تحتها الأرقام الثنائية المراد تحويلها إلى عشرية
كما في الصورة:

الأرقام الثابتة ←	١٢٨	٦٤	٣٢	١٦	٨	٤	٢	١
الرقم الثنائي المراد تحويله ←	١	١	١	١	٥	٥	٥	٥
	١٢٨	٦٤	٣٢	١٦	-	-	-	-

نلاحظ أننا تجاهلنا الأرقام التي تحتها صفر وأما ما تحته واحد هو الذي نقوم
بجمعه :. ١٦ + ٣٢ + ٦٤ + ١٢٨ = ٢٤٠
:. الرقم الثنائي 11110000 = الرقم العشري ٢٤٠

مثال٢ حول الرقم الثنائي 11111100 إلى رقم عشري

الحل

١٢٨	٦٤	٣٢	١٦	٨	٤	٢	١
١	١	١	١	١	١	٥	٥

٢٥٢ = ١٢٨ + ٦٤ + ٣٢ + ١٦ + ٨ + ٤ - -

الرقم 11111100 الثنائي = الرقم ٢٥٢ العشري

(مثال) حول الـ Ip الثنائي التالي إلى عشري 11000000.10101000.00000001.00110010

(الحل)

	١٢٨	٦٤	٣٢	١٦	٨	٤	٢	١	
octet1	1	1	0	0	0	0	0	0	= ١٩٢
octet2	1	0	1	0	1	0	0	0	= ١٦٨
octet3	0	0	0	0	0	0	0	1	= ١
octet4	0	0	1	1	0	0	1	0	= ٥٠

نجمع من كل octet ما تحته واحد ونتجاهل الذي تحته صفر فيبدأ الـ Ip

الثنائي 11000000.10101000.00000001.00110010 = الـ Ip العشري ١٩٢.١٦٨.١.٥٠

وهكذا تعلمنا كيفية التحويل من عشري Decimal إلى ثنائي Binary والعكس

لكن ما فائدة هذا التحويل ؟

الفائدة من هذا التحويل أن الداتا تمر في الكابلات على هيئة الرقم الـ Binary وكذلك رقم الـ Ip فنفرض أن الجهاز A يرسل إلى الجهاز B عنوان الـ Ip عند الجهاز المرسل يتحول إلى Binary ويمر في الكابلات إلى أن يصل إلى الجهاز المستقبل ويقوم كرت الشبكة في الجهاز B بتحويل الرقم من Binary إلى Decimal وهكذا تتم عملية نقل الداتا.

(ملاحظة هامة) عند تحويل الأرقام من عشري إلى ثنائي والعكس هناك أرقام سهلة نحفظها لتسهيل المسائل علينا وهي في الجدول

0	128	192	224	240	248	252	254	255
00000000	10000000	11000000	11100000	11110000	11111000	11111100	11111110	11111111

Subneting

① تحديد عدد الـ Host و الـ Subnetmask المناسب لها.

ذكرنا أنه منظمة الـ IANA قامت بتقسيم الايبهات إلى ٣ فئات

3 classes

class A (1 : 126) ← 255.0.0.0 مليون جهاز
class B (128 : 191) ← 255.255.0.0 ٦٥ الف جهاز
Class C (192 : 223) ← 255.255.255.0 ٢٥٤ جهاز

تخيل بفرض أن عدد أجهزة الشركة هو ٥٠٠ جهاز نريد أن نجمعهم في شبكة واحدة نجد أن class C لا يناسبهم لعدد أجهزة قليلة وكذلك class A/B مبالغ فيه أو هناك أعداد أجهزتهم بالنسبة لعدد الأجهزة لدى في العمل.

• في هذه الحاله نقوم بتحديد Subnetmask يناسب ذلك العدد من الأجهزة.

ابتداءً subnetmask = ٣٢ Bit وكي نقوم بتحديد Sunetmask مناسب لعدد الأجهزة نستخدم القانون التالي

$$hosts = 2^h - 2$$

والـ Host هو عدد الأجهزة

فهنا لدينا عدد أجهزة هو ٥٠٠ ∴ القانون $500 = 2^h - 2$

فنجد أنه أقرب أس يناسب أو يقارب الـ ٥٠٠ حيث يكون الأس هو ٩

$2^9 - 2 = 512 - 2 =$ **510**

أي عدد الأجهزة التي استطيع وضعها تحت الـ Subnetmask هي ٥١٠

الآن نستطيع معرفة الـ Subnetmask المناسب عن طريق اعتبار الـ h "الأس" عبارة عن أصفار، فنضع ٩ وهو الأس أصفار في الـ Subnetmask فنضع ٩ أصفار من اليمين وما بعدها يكون واحد كالتالي

11111111.11111111.11111110.00000000 فيكون عنوان الـ Subnetmask

هو ⟸ **255.255.254.0**

الخلاصة ⟸ عدد الأصفار في الـ Subnetmask يحدد عدد الأجهزة في هذه الشبكة عن طريق $host = 2^h - 2$ فعدد الأصفار ٩ ∴ $2^9 - 2 = 512 - 2 =$ **510 جهاز**

مثال آخر ماهو الـ Subnetmask المناسب لشركة بها 5000 جهاز ؟

الحل :

أفرض الـ Hosts = 5000

∴ $5000 = 2^h - 2$ حيث h هي عدد الأصفار في الـ Subnetmask

عن طريق استخدام الآلة الحاسبة نجد أن h = ١٣ حيث أقرب عدد قبله لـ 5000 هو ١٢ حيث أنه 2^{12} = ٤٠٩٦ وهذا غير مناسب ∴

∴ h = 13 ∴ $2^{13} - 2$ = ٨١٩٢-٢ هي هم الذين أستطيع وضعهم في شبكة واحدة.

فيكون لدي 13 صفر نضعهم من اليمين وما بعدهم نضعه واحد

11111111.11111111.11100000.00000000

ونحول الرقم الثنائي "Binary" إلى رقم عشري "Decimal"

سيكون 255.255.224.0 وهو الـ Subnetmask المناسب لعدد أجهزة ٥٠٠٠ حيث أنه يسمح بـ ٨١٩٠ جهاز في شبكة.

* تكلمنا في الأمثلة السابقة عن تحديد الـ Subnetmask ولم نتكلم عن الـ Ip والآن نتكلم عنه حيث في مثال الـ ٥٠٠٠ جهاز حددنا الـ Subnetmask وهو عنوان مهم ولكنه لم نتحدث عن عنوان الـ Ip كيف يتم تحديده للـ ٥٠٠٠ جهاز وهل كل الايبهات متاحة أم هل هناك ما لا أستطيع استخدامه ؟

لكي نقوم بإعطاء وتحديد عنوان لكل جهاز ولذلك لمعرفة المتاح لي كأدمن عند عنونة أجهزة الشركة نختار ابتداءً Ip عشوائي من ضمن الايبهات التي أود اعطائها للأجهزة. مثال نختار الـ Ip ١٠٠.١٠٠.١٠٠.١٥ بعد اختيار هذا الـ Ip نحدد عناصر الجدول التالي

Subnet	Fristvalid Ip	Lastvalid Ip	~~Subnetmask~~ Broad Cast ip

1 وال الخانة الأولى في الجدول هي الـ Subnet وهي تعني آخر Network address أي عنوان الـ IP الذي يأتي بعده كل أجهزة الشبكة ولكي يتم تحديد الـ Subnet هذا نقوم بتحويل الـ IP العنوان من عشري إلى ثنائي نجد أن الـ IP بالصورة الـ Binary هو

01100100 . 01100100 . 01100100 . 00001010

ثم نقوم بجمعه على الـ Subnet mask المناسب لـ ٥٠٠ جهاز كما في المثال الذي حددناه ونضع باعتبار (1+1=1) (1+صفر = صفر)

11111111 . 11111111 . 11100000 . 00000000
01100100 . 01100100 . 01100100 . 00001010

01100100 . 01100100 . 01100000 . 00000000

ثم نحول الناتج إلى عشري فيكون 100 . 100 . 96 . 0

∴ عنوان هذه الشبكة Network address أو ما يسمى Subnet هو

2 تحديد الـ Broad Cast IP

آخر خانة هي الـ Broad Cast IP وهو العنوان الذي عن طريقه نستطيع إرسال الداتا لكل الشبكة وهو آخر IP في الشبكة ولا نعطيه لأحد الأجهزة مثله مثل الـ Subnet حيث هو عبارة Network address وهو (-2) من القانون $2^n - 2 =$ hosts طريقة تحديده هي عن طريق الـ Subnet mask نضعه ونضع تحته الـ IP العنوان بالصورة الـ Binary

Subnet mask ← 11111111 . 11111111 . 111|00000 . 00000000

IP العنوان ← 01100100 . 01100100 . 011|00100 . 00001010

وعند آخر الواحايد في Subnet mask نفصل حاجزًا باللون الأحمر ما تحت الواحد من IP العنوان ينزل كما هو وما تحت الأصفار ينزل واحايد بالتالي ستكون النتيجة

ما تحت الواحد نزل كما هو ← 01100100 . 01100100 . 011 | 11111 . 11111111 | ← ما تحت الأصفار أصبح واحد

نقوم الآن بتحويل الـ Binary إلى Decimal سيكون 100.100.127.255

٣ | ١ | ما بين الـ Network address و الـ Subnet و الـ (Broadcast)
هى الأجهزة أو الأيبهات المتاحة فى الشبكة ويكون Frist valid Ip
هو أول ip و Last valid Ip هو آخر ip
لذلك الصورة النهائية للجدول هى :

Subnet	Frist valid Ip	Last valid Ip	Broad Cast
100.100.96.0	100.100.96.1	100.100.127.254	100.100.127.255

بعد تحديد المتاح لى من الايبهات أستطيع الآن عنونة أجهزة الشبكة واعطاء
ip لكل جهاز فكما ذكرنا الـ Subnet mask الذى هو 255.255.224.0 يستطيع
أن يجمع ٨١٩٠ جهاز فى هذه الشبكة .

٥ تحديد عدد الشبكات فى الـ Subnet mask

بفرض فى المثال السابق أن الشركة صاحبة الـ ٥٠٠ جهاز أرادت زيادة
أجهزة الشركة بعدد ٥٠٠ جهاز آخر أو حتى ١٠٠٠ جهاز نلاحظ
أن الـ Subnet mask يسع لـ ٨١٩٠ جهاز فى الشبكة فعند محاولة زيادة عدد الأجهزة
سوف أكون محكوم بعدد ٨١٩٠ فى الشبكة فما هى الطريقة التى نستطيع زيادة
عدد أجهزة الشركة ؟
بالطبع لا نستطيع أن نبدأ المسأله من جديد باعتبار ١٥٠٠ جهاز ونحسب الـ Subnet mask
والـ Hosts و الـ Valid Ip وهكذا لأن أجهزة الشركة سواء pcs أو راوترات
أو سيرفر الشركة أصبح له ip وبالتالى صعب جداً تغيرها فالحل فى ذلك
تكمن أن الـ Subnet mask نفسه يحتوى على أكثر من شبكة وكل شبكة بها
٨١٩٠ جهاز حسب المثال السابق كلم كيف يتم تحديدها ؟

نلاحظ أن الـ Subnet mask هو 11111111.11111111.11100000.00000000
نستطيع معرفة عدد شبكات الـ Subnet mask عن طريق معرفة عدد الوحايد فى

الـ octet الذي يحتوي على وحايد وأصفار أصبحين أو معه عدد الوحايد في الـ octet
الذي يحتوي على آخر واحد خاصة ... لدينا هو

11111111.11111111.11100000.00000000

الـ octet رقم ٣ هو الذي يحتوي على وحايد وأصفار وهو الذي يحتوي آخر
واحد فنحسب عدد الوحايد فيه نجد أنه ٣
نستخدم القانون ←

number of Subnet = 2^n

حيث أن number of subnets هي عدد الشبكات في الـ mask و (n) هي عدد الوحايد
في الـ octet الذي يحتوي أصفار ووحايد أو به آخر واحد.

∴ $2^3 = 8$ ∴ هذا الـ mask يحتوي على عدد شبكات فرعية [٨]

ولكي نحدد بداية كل شبكة نستخدم Blocksize ونستطيع تحديده عن طريق
ما يقابل آخر واحد في الـ Subnetmask من الأرقام الأساسية |١ ٢ ٤ ٨ ١٦ ٣٢ ٦٤ ١٢٨|
فنجد أن آخر واحد يقابله [٣٢] فنزيد في الـ octet الثالث مقدار الـ Blocksize
نزيد ٣٢ في كل عنوان شبكة فيصبح الجدول

Subnet	Frist valid Ip	Last valid Ip	Broadcast
100.100.96.0	100.100.96.1	100.100.127.254	100.100.127.255
نزود ٣٢ على الـ octet الثالث في كل صف			
100.100.128.0	100.100.128.1	100.100.159.254	100.100.159.255
100.100.160.0	100.100.160.1	100.100.191.254	100.100.191.255

ومنه لدي ٨ شبكات في هذا الماسك (mask) لكن كل شبكة
لا ترى الأخرى إلا عن طريق استخدام راوتر

* كل شبكة تحتوي على ٨١٩٠ جهاز

هام: اتضح لي من الأمثلة السابقة أنني أستطيع تحديد عدد الأجهزة عن طريق عدد الأصفار في الـ Subnet mask في حين أنني أستطيع تحديد عدد الشبكات في الـ subnet mask عن طريق عدد الوحايد

عدد الأجهزة = $2^n - 2$ حيث n هي عدد الأصفار

عدد الشبكات = 2^n حيث n "Networks" هي عدد الوحايد في الـ octet الذي يحوي وحايد وأصفار أو الذي يحوي آخر واحد في الـ subnet mask

الخلاصة الـ Subnet mask يتضمن جزئين جزء يمثل الشبكة Network وهي البتات ذات القيمة 1 وجزء يمثل الأجهزة الـ Hosts وهي البتات ذات القيمة 0

class C	Network Bits	Hosts Bits
	11111111.11111111.11111111	00000000

شراء IP

يستطيع الإنسان أن يعطي أجهزة الشركة الخاصة به عناوين IP دون أن يقوم بدفع أي مبلغ من المال لكن في هذه الحالة لن يستطيع الاتصال بشبكة الانترنت هذا النوع هو الـ private IP وهو داخل الشركة ولا أستطيع عن طريقه استخدامه الدخول إلى الانترنت.

الـ public IP ⇐ هو نوع آخر من IP يقوم صاحب الشركة بشرائه من مزود الخدمة مثل شركة المصرية للاتصالات عن طريق هذا الـ IP نستطيع الدخول على الانترنت

* بالطبع قد لا يختلف عنوان Private عن آخر public لكن الأخير الذي تقدمه الشركة المزودة للخدمة هو الذي يساعدنا للدخول للإنترنت.

مصطلح الـ CIDR

الـ cidr هو العملية العكسية لـ Subneting وهو إختصار لكلمة Classless Inter-Domain Routing ويسمى أيضاً "Superneting".

وبإختصار هو البلوك الذي أحصل عليه وابدأ في تقسيم الشبكات بناءً عليه سواء من حيث عدد الأجهزة أو عدد الشبكات.

• شكل الـ cidr ← مثال ← 205.5.5.0/24

الجزء الأول من هذا الـ cidr [205.5.5.0] هو عبارة عن الـ Subnet أو بمعنى آخر هو عنوان الشبكة Network Id وأما الجزء الثاني من الـ cidr وهو الرقم [24] كما في المثال فإنه عبارة عن الـ Subnetmask فهو بمعنى آخر يمثل عدد الوحدات ذات القيمة (1) في الـ Subnetmask

(مثال آخر)

Networkaddress ← 176.7.0.0/16 → Subnetmask

تمارين على الـ Subneting

[مثال ١] لديك الـ cidr ← 205.5.5.0/24 والمطلوب منك تقسيمه إلى ٧ شبكات وتحديد الـ Networkaddress و Broadcast و valid Ips لكل شبكة؟

(الحل)

أولاً نعرف قيمة الـ Subnetmask في الـ cidr الـ IP من الكلاس C

عدد الشبكات = ٢ⁿ ∴ ٧ = ٢ⁿ ∴ ن = ٣

∴ نزيد عدد الوحايد في الماسك الأصلي بقيمة ٣ وحايد

11111111.11111111.11111111.11100000

ونقوم بالتحويل من ثنائي لعشري سيكون

255.255.255.224

فتكون أول شبكة من الـ ٧ شبكات

الـ cidr الأساسي ← Network

205.5.5.0/27 ← الماسك الجديد.

ونحدد البلوك سايز أو ما يدعى "step" وهو قيمة أخر واحد في الـ octet المختلط أو الذي به آخر واحد

~~الشبكة الأولى 205.5.5.0/27~~

~~الشبكة الثانية~~

يكون الـ step = [32]

∴ الشبكة الأولى هي 205.5.5.0/27

هو Frist Valid Ip 205.5.5.1

هو Last Valid Ip 205.5.5.30

هو Broad Cast 205.5.5.31

وعرفنا الـ Broadcast للشبكة الأولى عن طريق زيادة الـ step وهو ٣٢ في الشبكة الأولى في الـ octet الأخير فتكون الشبكة الثانية هي 205.5.32 ونطرح منها يكون Broadcast الشبكة التي قبلها.

	Networkaddress	valid	BroadCast
الشبكة الثانية	205.5.5.32/27	(5.33 : 5.62)	5.63
الشبكة الثالثة	205.5.5.64/27	(5.65 : 5.99)	5.95
الشبكة الرابعة	205.5.5.96/27	(5.97 : 5.126)	5.127
الخامسة	205.5.5.128/27	(5.129 : 5.159)	5.160
السادسة	205.5.5.160/27	(5.161 : 5.191)	5.192
السابعة	205.5.5.192/27	(5.193 : 5.122)	5.123

مثال مطلوب ٣٠٠ شبكة مع العلم أن الـ Cidr هو 167.7.0.0/16

الحل

∵ عدد الشبكات المطلوبة = ٢ⁿ

∴ ٣٠٠ = ٢ⁿ ∴ n = ٩

حيث يكون لدينا ٥٠٠ جهاز وهو أقرب شيء يمكن الحصول عليه مقارب لـ ٣٠٠ جهاز

نقوم الآن بإضافة ٩ وحايد للماسك للحصول على الماسك الجديد

11111111.11111111.11111111.10000000

∴ الماسك الجديد هو 25 ∴ الشبكات الأولى هي [167.7.0.0/25]

نقوم الآن بحساب الـ step أو ما يسمى الـ Blocksize عن طريق معرفة ما يقابل آخر واحد من البتات الوحايد من الماسك الجديد نجد أن المقابل له 128

∴ نزيد ١٢٨ في الـ octet الأخير حيث أنه مكان آخر واحد حتى نحصل على الشبكات الأخرى

167.7.0.0/25	الشبكة الأولى
167.7.0.128/25	الشبكة الثانية
167.7.1.0/25	
167.7.1.128/25	
167.7.2.0/25	

وهكذا إلى أن نصل إلى ٣٢ شبكة.

مثال ٣ مطلوب ٢٠٠ شبكة مع العلم أن الـ Cidr هو 12.0.0.0/8

الحل

عدد الشبكات = 2^n ∴ $2^n = 200$

∴ n = 8 حيث الناتج هو 256 أقرب شيء لـ 200 جهاز

إذن نزيد ٨ وحايد في الماسك الجديد

11111111.11111111.00000000.00000000

∴ الماسك الجديد هو ١٦ والشبكة الأولى هي 12.0.0.0/16

الآن نقوم بحساب الـ step وهو آخر صفر في الماسك ونجد ما يقابله هو ① فنزيد الـ octet الثاني حيث هو مكان آخر واحد بمقدار ①

∴ الشبكات هي

12.0.0.0/16	الشبكة الأولى
12.1.0.0/16	الشبكة الثانية
12.2.0.0/16	الشبكة الثالثة
12.3.0.0/16	الشبكة الرابعة

وهكذا إلى أن نصل إلى ٢٠٠ شبكة.

مثال: لدينا الـ 210.10.10.0/24 Cidr تم بتقسيمه إلى شبكات بحيث يكون في كل شبكة ٦٠ جهاز؟

الحل

هذه المسألة المطلوب فيها ليس عدد شبكات لكن أن يكون في كل شبكة ٦٠ جهاز ∴ نستخدم القانون $Hosts = 2^h - 2$

∴ عدد الأجهزة $= 2^h - 2$

$60 = 2^h - 2$

نجد أن $h = 6$ حيث سيكون الناتج $2^h = 2^6 = 64$ جهاز

$64 - 2 = 62$ أي أن الشبكات أفضل ما يمكن تقسيمها إليه هو ٦٢ جهاز في كل شبكة.

* لكي نقوم بتحديد الماسك الجديد نضع h عبارة عن أصفار، أي أننا سنضع ٦ أصفار، والباقي وحايد

11111111.11111111.11111111.11000000

وهو 255.255.255.192

∴ الماسك الجديد زاد فيه عدد الوحايد بمقدار ٢ ∴ سيكون **26**

∴ الشبكات هي

210.10.10.0/26 الشبكة الأولى

210.10.10.64/26

210.10.10.128/26

210.10.10.192/26

كل شبكة سيكون بها ٦٢ جهاز والناتج ٤ شبكات فقط حيث أن عدد الوحايد في الـ octet الأخير صاحب آخر واحد هو ٢

عدد الشبكات $= 2^n = 2^2 = 4$ شبكات.

مثال ٥ مطلوب ٥٠٠ جهاز في كل شبكة مع العلم أن الـ cidr هو 172.16.0.0/16

الحل

عدد الأجهزة = $٢^n - ٢$

$٥٠٠ = ٢^n - ٢$

$٥٠٠ = ٢^٩ - ٢$

$٥٠٠ = ٥١٢ - ٢ = ٥١٠$

∴ علينا أن نضع ٥١٠ جهاز في الشبكة الواحدة.

نقوم الآن بوضع ٩ أصفار في الـ mask الجديد

11111111.11111111.11111110.00000000

∴ الـ mask الجديد هو 23

نحدد الآن الـ step وهو قيمة ما يقابل آخر واحد نجد أنه ٢

∴ ستزيد قيمة الـ octet الثالث بمقدار ٢

∴ الشبكات هي:

172.16.0.0/23 الشبكة الأولى

172.16.2.0/23

172.16.4.0/23

172.16.6.0/23

حتى يصبح لدينا عدد من الشبكات نستطيع حسابه عن طريق ٢^n حيث n هي عدد الوحايد في الـ octet الثالث = $٢^٧$ = 128 شبكة.

مثال ٦ إذا كان الـ cidr هو 10.0.0.0/8 مطلوب تقسيمه إلى شبكات بحيث يكون ١٠٠٠ جهاز في كل شبكة.

الحل

عدد الشبكات = $٢^n - ٢$ ∴ $١٠٠٠ = ٢^n - ٢$

∴ n = ١٠ ∴ ١٠٠٠ = ١٠٢٤ - ٢ = ١٠٢٢ جهاز في الشبكة.

نحول الآن الـ n إلى أصفار في الـ mask الجديد.

11111111.11111111.11111100.00000000

∴ عنوان الماسك الجديد هو (22)

نقوم الآن بحساب الـ step نجد أنه = 4

∴ الشبكات هي

10.0.0.0/22	الأولى
10.0.4.0/22	الثانية
10.0.8.0/22	الثالثة
10.0.12.0/22	الرابعة

ويكون لدينا عدد شبكات يمكن حسابه عن طريق

عدد الشبكات = 2^n حيث n هي عدد الزيادة في البتات الوحايد عن

الماسك الأصلي أو بمعنى أخر الوحايد الزيادة في الماسك الجديد.

عدد الشبكات = 2^{15}

عدد الشبكات = ٣٢,٧٦٨ شبكة

VLSM

الـ VLSM هي اختصار Varible length subnet mask وهي عملية يتم من خلالها تقسيم الشبكة الرئيسية " cidr " إلى عدد من الشبكات الفرعية غير المتساوية من حيث عدد الـ Hosts بخلاف الـ Subneting الذي يكون فيه عدد الـ Hosts متساوي في كل شبكة فرعية، ويتم ذلك عن طريق جعل الـ Subnetmask متغير في كل شبكة فرعية

مثال إذا كان الـ cidr هو 192.168.10.0/24 نريد تقسيم هذا الـ cider إلى ٥ شبكات الأولى بها ١٠٠ جهاز والثانية ٥٠ والثالثة ٣٠ والرابعة والخامسة لكل منهما ٥ أجهزة فما هي الطريقة ؟

الحل نقوم بتقسيم هذا الـ cidr إلى أكثر من Subnetmask ويتم ذلك

باعتبار كل عدد مطلوب من الأجهزة شبكة منفصلة

① الشبكة الأولى ١٢٠ جهاز

عدد الأجهزة = $٢^{ن} - ٢$ ∴ ١٢٠ = $٢^{ن} - ٢$

١٢٠ = $٢^{٧} - ٢$ ∴ ١٢٠ = ١٢٨ - ٢ = ١٢٦

∴ أقرب ما يمكن وضعه للشبكة هو ١٢٦

نضع الآن ٧ أصفار لتحديد الماسك الجديد

11111111.11111111.11111111.10000000

∴ الماسك الجديد هو 25

∴ الشبكة الأولى هي 192.168.10.0/25

والـ step هو ١٢٨ قيمة ما يقابل آخر واحد

∴ الشبكة الثانية عنوانها هو 192.168.10.128

② الشبكة الثانية ٥٠ جهاز

عدد الشبكات = $٢^{ن} - ٢$ ∴ ٥٠ = $٢^{٦} - ٢$ ∴ ٥٠ = ٦٤ - ٢ = ٦٢

عدد الأجهزة في الشبكة ٦٢

نضع ٦ أصفار لتحديد الماسك الجديد

11111111.11111111.11111111.11000000

∴ الماسك لهذه الشبكة هو 26

∴ الشبكة هي 192.168.10.128/26

نحدد الـ step نجد أنه ٦٤

∴ الشبكة الثالثة هي 192.168.10.192

③ الشبكة الثالثة ٣٠ جهاز

٣٠ = $٢^{ن} - ٢$ = $٢^{٥} - ٢$ = ٣٢ - ٢ = ٣٠

نضع ٥ أصفار لتحديد الماسك الجديد

11111111.11111111.11111111.11100000

∴ الماسك لهذه الشبكة هو [27]

∴ الشبكة هي 192.168.10.192/27

نحدد الآن ال step نجد أنه [٣٢]

∴ الشبكة التالية هي 192.168.10.224

الشبكة الرابعة: ٥ أجهزة عنوان 192.168.10.224

$٥ = ٢^ن - ٢$ ∴ $٥ = ٢^٣ - ٢ = ٨ - ٢ = ٦$

∴ عدد الأجهزة = ٦ في الشبكة

نضع الآن ٣ أصفار للماسك الجديد

11111111.11111111.11111111.11111000

∴ الماسك الجديد هو 29 ∴ الشبكة هي 192.168.10.224/29

ونحدد ال step نجد أنه [٨]

∴ الشبكة التالية هي 192.168.10.232

الشبكة الخامسة

$٥ = ٢^ن - ٢ = ٥ = ٢^٣ - ٢ = ٨$

الماسك لهذه الشبكة هو [29]

∴ الشبكة هي 192.168.10.132/29

∴ إجمالي الشبكات

1. 192.168.10.0/25
2. 192.168.10.128/26
3. 192.168.10.192/27
4. 192.168.10.224/29
5. 192.168.10.232/29

مثال: إذا كان لديك cidr هو 223.10.10.0/24 والمطلوب هو تقسيمه إلى ٣ شبكات الأولى ٥٠ جهاز والثانية ١٠ أجهزة والثالثة هي الشبكة الواصلة بين الشبكتين وتحتوي على ٢ IP فقط ما هو الحل؟

(الحل)

ال cidr هو 223.10.10.0/24

١) الشبكة الأولى ٥٠ جهاز

$hosts = 2^h - 2$

$50 = 2^6 - 2$

$50 = 64 - 2$

$hosts = 62$

الحد المسموح به هو ٦٢ جهاز في هذه الشبكة ∴ نقوم الآن بزيادة أو وضع ال ٦ أصفار والباقي وحايد للحصول على الماسك الجديد.

Newmask = 11111111.11111111.11111111.11000000

∴ الشبكة الأولى تبدأ 223.10.10.0/26

نحسب الآن ال step نجد أنه = 64 حيث = 2^h أو ما يقابل آخر واحد

∴ بداية الشبكة الثانية هي 223.10.10.64

٢) الشبكة الثانية بدايتها هي 223.10.10.64 ومطلوب ١٠ أجهزة

$hosts = 2^h - 2$ ∴ $10 = 2^4 - 2$ - hosts = 14

الحد المسموح به 14 جهاز ∴ نضع الآن ٤ أصفار والباقي وحايد.

Newmask = 11111111.11111111.11111111.11110000

∴ الشبكة هي 223.10.10.64/28

نقوم بحساب ال step = 2^h = 2^4 = 16

∴ الشبكة الثالثة هي 223.10.10.80

٣) الشبكة الثالثة بدايتها 223.10.10.80 وعدد أجهزتها ٢

$hosts = 2^h - 2$ $2 = 2^2 - 2$ $2 = 4 - 2 = 2$

∴ Newmask = 11111111.11111111.11111111.11111100

الشبكة الثالثة هي 223.10.10.80/30
الشبكة الثالثة ستبدأ بـ ← 223.10.10.80 حيث الـ step = 4

	Network ID	Frist valid Ip	Last valid Ip	BroadCast
الشبكة الأولى	223.10.10.0/26	223.10.10.1	223.10.10.62	223.10.10.63
الشبكة الثانية	223.10.10.64/28	223.10.10.65	223.10.10.78	223.10.10.79
الشبكة الثالثة	223.10.10.80/30	223.10.10.81	223.10.10.82	223.10.10.83

class D & E

لاحظنا أن منظمة الـ IANA قامت بتقسيم الايبهات إلى classes ذكرنا منها C & B & A

* لكن هناك class D وهو (224 - 239) أي أن أي Ip يبدأ الـ octet الأول منه برقم من ٢٢٤ إلى ٢٣٩ فهو class D وهو خاص بالـ multiCast ← ليس مقرر على CCNA والـ multiCast يختلف عن الـ BroadCast حيث أن الأخير استطيع إرسال الداتا لكل أجهزة الشبكة في حين أن الـ multiCast يرسل الداتا لجزء معين من الشبكة.

* classE ← (240 : 255) هذا الـ class أنشئ للاستخدام المستقبلي لكن نتيجة التوسع في استخدام الأيبهات ظهر جيل جديد من الايبهات هو Ipv6

The Ip 127.0.0.1

لاحظنا أن classA (1 : 126) و classB (128 : 191)
نا ير ذهب الـ Ip الذي رقمه 127 ؟
يستخدم هذا الـ Ip (127) في عملية يطلق عليها LoopBack

ويطلق عليه أيضاً Localhost وعن طريق هذا الـ Ip نقوم بعمل فحص لجهاز الكمبيوتر هل بروتوكول Tcp/ip معرف على الجهاز أم غير معرف وبمعنى آخر هل كارت الشبكة معرف على الكمبيوتر أم غير معرف نستطيع التأكد من ذلك عن طريق الدخول على أمر cmd ونكتب ping 127.0.0.1 إذا أعطاني replay فإذاً البروتوكول معرف وكذلك كرت الشبكة معرف
أي أن هذا الـ Ip 127 يستخدم في عملية الـ Troubleshooting.

مهارات في الـ Subneting

قد يعطيني في الاختبار مجموعة من الايبهات في شبكة واحدة ويطلب مني أن أجد أنسب Subnetmask لهذه الايبهات.

مثال لدينا هذه المجموعة من الايبهات
10.0.200.200 } 10.0.180.5 } 10.0.20.200 } 10.0.0.5
فما هو الـ Subnetmask المناسب لهم.؟

(الحل)

① لمعرفة الـ Subnetmask المناسب لهم نحدد أصغر Ip وأكبر Ip عن طريق معرفة رقم الـ octet غير الثابت في كل Ip فنجد أن الجزء 10.0 ثابت في كل Ip ويبدأ الاختلاف في الـ octet الثالث ∴ أصغر Ip هو 10.0.0.5 وأكبر Ip هو 10.0.200.200

② نقوم بتحويل الـ octet الذي حددنا على أساسه أصغر Ip إلى Binary

أصغر Ip ← 0 = 00000000
أكبر Ip ← 200 = 11001000

③ ننظر للبت رقم 1 إذا كان فيه تشابه سواء صفر مع صفر أو واحد مع واحد ينزل الرقم 1 ونكمل للبت التالي لو تشابه ينزل واحد وهكذا لكن إذا اختلف البت سواء صفر مع واحد أو واحد مع صفر ينزل هو وكل ما بعده أصفار

∴ 00000000
11001000

00000000 ← اختلف البت الأول من كل Ip فننزل الكل أصفار

∴ الـ Subnetmask المناسب هو

255.255.0.0

مثال آخر: لديك المجموعة التالية من الايبهات ماهو الـ Subnetmask المناسب لهم؟

10.0.5.200 ، 10.0.10.5 ، 10.0.2.200 ، 10.0.7.5

الحل

① تحديد أصغر وأكبر Ip

الأصغر هو 10.0.2.200

الأكبر هو 10.0.10.5

② نقوم بتحديد الـ octet الأول بعد الثوابت نجد أنه الـ octet الثالث ونقوم بتحويله إلى Binary

الأصغر = 2 = 00000010

الأكبر = 10 = 00001010

③ ما كان متشابه يتنزل واحد ولو اختلفا ينزل وما بعد أصفار

∴ الناتج هو 11110000

∴ الـ Subnetmask المناسب هو

255.255.240.0

الـ 255.255 يمثل الجزء المشترك من جميع الايبهات وهو 10.0

مثال من نوع آخر

قد يعطيني في الاختبار عنوان شبكة مثل 192.115.103.64/27 ويطلب مني الـ Network ID التالي لهذه الشبكة.

الحل

نقوم بتحويل الـ Subnetmask إلى وحايد وأصفار :-

11111111.11111111.11111111.11100000

نقوم الآن بتحديد الـ step وهو 2^h حيث h هي عدد الأصفار، ممكن تحديدة أيضاً عن طريق معرفة مايقابل آخر واحد من مضاعفات الـ 2

$\therefore step = 2^5 = 32$ $\therefore$ نضيف 32 في الـ octet الأخير

$\therefore$ الـ NetworkID التالي هو

192.115.103.96/27

هكذا نكون انتهينا من جزء Ip Subneting / VLSM

القوانين المستخدمة في هذا الباب

① Number of hosts $= 2^h - 2$

حيث h هي عدد الأصفار

② number of Networks $= 2^N$

حيث N هي عدد الوحايد الزائدة على الماسك الأصلي

③ BlockSize "step" $= 2^h$

حيث h هي عدد الأصفار في الـ octet المنسب أصفار ووحايد أو بمعنى آخر الذي فيه عليه ويمكن حسابه عن طريق معرفة مايقابل آخر واحد في الماسك الجديد.

The Routing

The Routing

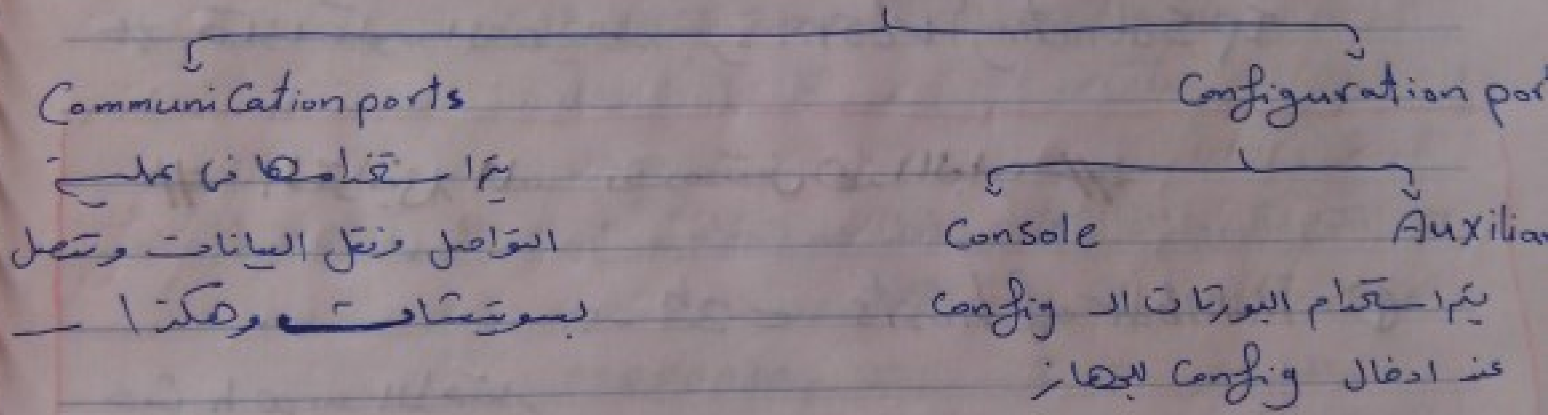
The Routing

سابقاً كان هناك باب مخصص في راوترز سيسكو وانواعها لكنه مع تقدم الشركة وتصنيع أكثر من روتر اصبح الكلام الآن على أساسيات كل راوتر.

يتكون كل راوتر من

① CPU معالج
② RAM ← يتم تخزين الاعدادات عليها لحين نقلها إلى الذاكرة الغير متطايرة.
③ Flash memory ← يتم حفظ الـ IOS Image
④ NVRam ← يتم حفظ الـ Config عليها ولا تفقد بانقطاع التيار.
⑤ Rom ← معلومات عامة عن الراوتر

بورتات الراوتر



* يمكن إضافة موديول عند الاحتياج سواء موديول ethernet أو سيريال.

* Serial port ⟸ هي منفذات تتميز بأنك تستطيع التحكم في السرعة حيث أنه في الـ ethernet يمكن التحكم فيه بتقليل السرعة ١٠ ميجا أو نجعلها ١٠٠ ميجا لكن السيريال تتحكم فيه بأي سرعة مثل 128KB و 500KB و هكذا.
وأيضاً نعتمد السيريال تربط بين الشبكات الواسعة الـ Wan
وأيضاً عن طريقه يتم توزيع سرعة من الراوتر إلى راوتر آخر وتسمى تقنية Back to Back

وكابلات السيريال تنقسم إلى

mail
(DTe)
Data Terminal equipment

Femail
(DCe)
Date Communication equipment

* الاسم السوقي لكابل السيريال V.35
* يتم توصيل الكابل الـ Femail في الراوتر صاحب الشبكة العضوي "راوتر TEdata"
* يتم توصيل الكابل الـ mail في الراوتر الذي يستقبل ما يتم توزيعه عليه "الشبكات الصغرى"

Router Configuration

تتشابه أوامر الراوتر مع أوامر السويتش في بعض الـ Configuration وهي

① الدخول للجهاز — >en
② الدخول لـ privileged — #
③ الدخول لـ global Configuration — (Config) #
④ تفعيل الباسوورد واستخدام الـ Console & Telnet . SSH
⑤ تغيير اسم الجهاز والعادات البانر
⑥ تحديد البورت وأوامر الـ Help
⑦ أوامر الـ Save وبعض أوامر الـ Show.

لمراجعة هذه الـ Config نراجعها في باب السويتش.

تحديد الـ Getway

ابتداءً إذا كان لدي أكثر من شبكة فأستطيع أن أعمل Communication بين هذه الشبكات عن طريق الراوتر وإعطاء كل بورت Ip من الشبكة المتصله به هذا الـ Ip هو الـ Getway لهذه الشبكة.

مثال: البورت F0/0 نريد أن نجعله ال getway للشبكة 192.168.10.0

الإجابة:

```
Router > en
Router # Config T
Router(config) # int F0/0
Router (config-if) # No shutdown
Router (config-if) # ip address 192.168.10.1 255.255.255.0
```

* وغالبا نعطي ال getway آخر ip في الشبكة أو أول ip وهذا للتسهيل عند تذكرهم في حالة النسيان.
* نستطيع متابعة حالة ال interface عن طريق الأمر show Ip interface Brief

vlan getway

الطريقة السابقة كانت الطريقة في حالة الشبكة العادية فكل شبكة تأخذ getway من الشبكة ونعطيه للبورت الواصل عليه هذه الشبكة. لكن في حالة الـ Vlan يختلف الأمر حيث تقوم ال vlan بتقسيم الشبكات إلى شبكات وهمية وبالتالي كل vlan ستحتاج إلى getway في حين أن كل ال Vlan تكون متصله على بورت واحد. فما هو الحل.

① الطريقة باستخدام الراوتر

① نجعل البورت في السويتش الذي يتصل بالراوتر Trunk
② بالنسبة لبورت الراوتر نجعله up عن طريق أمر No shutdown
③ نقسم البورت إلى Subinterfaces ونعطي كل (Subint) Ip من ال vlan

مثال: لدي شبكتين Vlan الاولى Vlan10 والثانية Vlan20 وهما متصلتين على البورت F0/1 في الراوتر ونريد اعطائهما getway فما هو الحل.

الاجابه

① تحديد البورت في السويتش المتصل بالراوتر Trunk

switch(config-if)# switchport mode Trunk

② فتح البورت في الراوتر " Fo/1 "

Router >en
Router # Config T
Router(config) # int Fo/1
Router (Config-if)# No Shutdown

③ تقسيم الـ interface إلى Subinterface

Router(config) # int Fo/1 . ___ أي رقم

١- vlan10

Router(config) # int Fo/1 . 10 ← أي رقم
Router (config-Subif) # encapsulation dot1Q ___ 10 اسم الـ vlan
Router (config-subif) # ip address ___ ip الـ vlan 10

٢- vlan20

Router(config) # int Fo/1 . 20 → أي رقم
Router(config-Subif) # encapsulation dot1Q ___ 20 → رقم الـ vlan
Router(config-Subif) # ip address ___ ip الـ vlan رقم ٢٠

* لمتابعة ماتم عمله من الـ Configuration ← Show Ip Route.

④ باستخدام Layer 3 Switch

يتميز الـ layer 3 switch بأنه يعمل راوتر وسويتش وهذه ميزة وتفضيل.

عمل الـ getway لـ ← vlans

① مشكلات المعاشة ولشبكة الـ vlan

```
switch (config) # int F0/1
switch (config-if) # No Switchport
switch (config-if) # Ip addlress : ____ IP ____
```

② للـ vlans

```
switch (config) # interface vlan __ex__ → اسم الـ vlan
switch (config-vlan) # No shutdown
Switch Router (config-vlan) # ip addlress ____ ex ____
```

ونعمل الخطوة هذه في كل vlan

تفعل الـ Routing على السويتش لكي يعمل Routing لأنه يعمل Layer3 switch

```
switch (config) # ip Routing
```

ولا تنسى أن ندخل على أجهزة الشبكة تعمل عليها الـ getway

Route types

Dynamic | STatic

static Route [1]

يتم تعريف الشبكات بطريقة يدوية لا تستخدم البروتوكولات (ميزاته)

① لا تحتاج لامكانيات هائلة ② أكثر أمانا

حيويه ⊙ يستخدم في الشبكات الصغيرة ⊙ آلية مرهقة لأنظمة الكتابة والـ config

* بداية عند كتابة أمر show Ip Route يظهر لنا الشبكات التي يتعرف عليها ويظهر أمامها حرف الـ C وهو اختصار كلمة Connected وهي الشبكات المتصلة بالراوتر اتصال مباشر. الشبكات الغير متصلة اتصال مباشر عند تعريفها تظهر أمامها نوع التعريف سواء static سيظهر حرف S وإذا كان Dynamic يظهر اختصار البروتوكول المستخدم

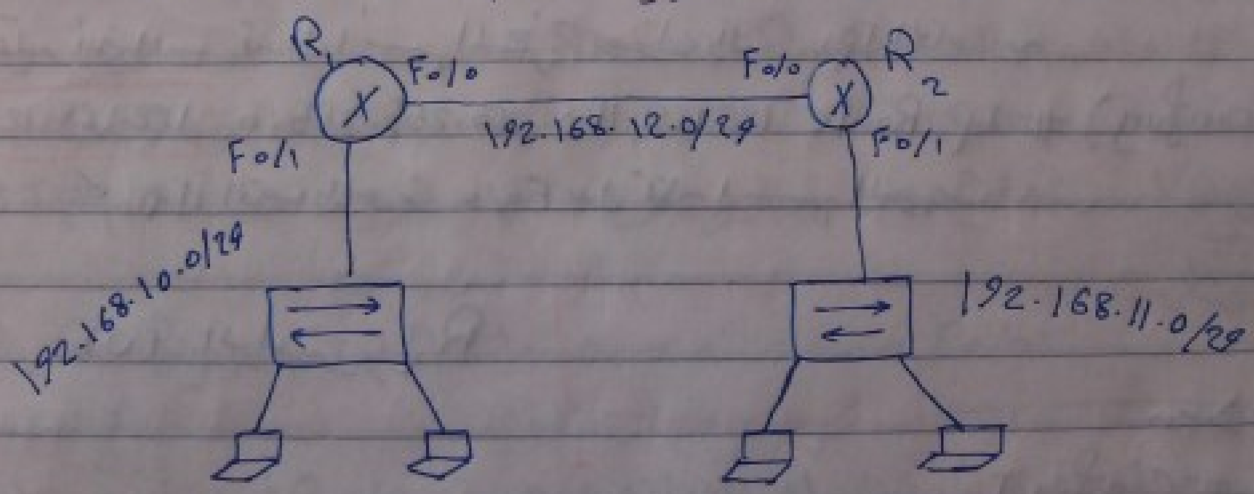
Static Configuration

ندخل على الراوتر ونحدد الشبكة التي نريد تعريفها عليه والتي بالطبع ليست متصلة به اتصال مباشر ونقوم بتعريفها عن طريق الأمر التالي

Router(config) # Ip Route ______ ______ ______

(IP: الخاص بالشبكة المراد تعريفها — SM: الخاص بالشبكة المراد تعريفها — اسم البورت أو IP البورت)

مثال: لدينا جهازين راوتر R_1 و R_2 لكل منهم شبكة لها عنوانه كما في الرسم والشبكة بين الراوترين كما بالرسم كيف نعرف كل شبكة متصلة على راوتر للجهاز الآخر لكي يتم الاتصال بين أجهزة الشبكات عن طريق استخدام الـ Static Route.



الإجابة

① أولا سنعرف كل شبكة ونعطيها getway وهو الـ Ip الذي سيحصل عليه المخرج المتصل بالشبكة من كل راوتر ونكتب الـ getway لكل جهاز في الشبكة الخاصة به

٥ المخارج بين الراوترين تأخذ عنوان Ip من الشبكة بين الراوترين
فيكون لدينا مخارج كل راوتر على النحو التالي

R_1

Fo/o = 192.168.12.1/24

Fo/1 = 192.168.10.1/24 ← وهو يمثل getway الشبكة المتصلة به

R_2

Fo/o = 192.168.12.2/24

Fo/1 = 192.168.11.1/24 ← وهو الـ getway للشبكة المتصلة به

---

٣ نعمل الآن الـ static Route

(أ) الراوتر R_1

```
R1>en
R1# Config T
R1(config)# Ip Route 192.168.11.0 255.255.255.0 Fo/o
```

Ip Route ← أمر الـ Route

192.168.11.0 255.255.255.0 ← الشبكة المراد تعريفها للراوتر

Fo/o ← المخرج الذي عن طريقه نصل الشبكة

* يمكنه أيضاً استبدال اسم المخرج بعنوان الـ Ip الخاص به

```
R1(config)# Ip Route 192.168.11.0 255.255.255.0 192.168.12.1
```

↙ Ip الخاص بالبورت Fo/o بدل كتابة اسم البورت.

(ب) الراوتر R_2

```
R2>en
R2# Config T
R2(config)# Ip Route 192.168.10.0 255.255.255.0 Fo/o
```

أو 192.168.12.2

Ip Route ← أمر الراوتنج

192.168.10.0 255.255.255.0 ← الشبكة المراد تعريفها.

Fo/o ← البورت الذي نصل من خلاله للشبكة.

بعد كتابة الـ Configuration نتابع الذي ما قمنا به

R1 # Show Ip Route

سيظهر لنا

C	192.168.10.0/24	Connected
C	192.168.12.0/24	Connected
S	192.168.11.0/24	Static

الـ Connected هي الشبكات المتصلة بالراوتر مباشرة.

الـ Static الشبكات التي تم تعريفها للراوتر عن طريق الـ Static Route

R2 # Show Ip Route

C	192.168.11.0/24	Connected
C	192.168.12.0/24	Connected
S	192.168.10.0/24	Static

وهكذا تكويناتهما على المثال.

---

* لإلغاء الـ Static Route نسبق الأمر بكلمة No

R2(Config) # No Ip Route ___ ex ___ . F___

خاصية الـ Default Route

هنا في الـ Static يكون لا نكتب اسم الشبكة المراد تعريفها للراوتر ولكن نعرف الراوتر على أي شبكة يكون الوصول إليها عبر البورت عن طريق استخدام Default Ip

مثال

R1 (Config) # Ip Route 0.0.0.0 0.0.0.0 F0/0

معناها أي شبكة لا تمتلك طالما أنها على البورت F0/0 أو بمعنى آخر نصل إليها عن طريق الخروج منه فالراوتر سيعمل لها Route وتسمى هذه الطريقة الـ Default Route

الـ Nexthop

لاحظنا أننا نكتب اسم البورت أو عنوان الـ IP الخاص به بالنسبة للراوتر الذي نكتب على الـ Configuration هنا البورت يسمى exit port أي الذي تخرج منه الداتا

Nexthop ← هو البورت المقابل في الراوتر الآخر الذي يتصل ببورت الجهاز الذي نعمل على الـ Config ونستطيع استبداله على الـ config.

(مثال)

R1(config)# Ip Route 192.168.11.0 255.255.255.0 192.168.12.1

✓ هذا هو exit port للراوتر R1 يمكن استبداله وكتابة البورت المقابل له في الجهاز R2 ليكون الأمر

R1(config)# Ip Route 192.168.11.0 . 255.255.255.0 192.168.12.2

✓ هذا هو عنوان الـ IP لـ Nexthop

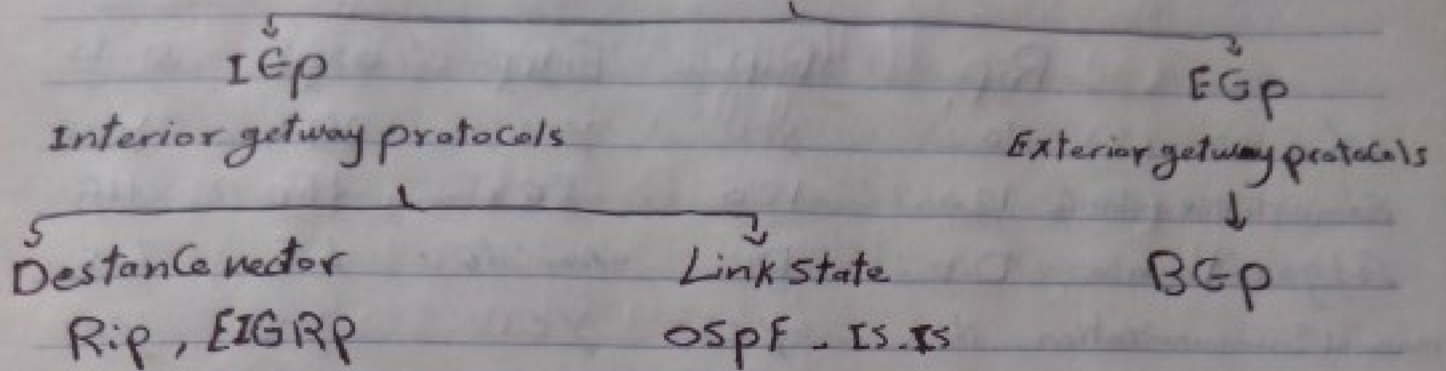
Dynamic Route 2

هو استخدام البروتوكولات في عملية الـ Routing

يقوم الـ DynamicRoute بعملية استكشاف الشبكات في أجهزة الراوتر المجاورة عن طريق Hello و advertising

الـ Hello ← يقوم الراوتر بإرسالها لمعرفة الأجهزة التي تستخدم نفس البروتوكول. ويتم الرد من الراوترز التي تستخدم نفس البروتوكول

الـ advertising ← عند التعرف على الأجهزة التي تستخدم نفس البروتوكول يقوم كل جهاز بإعلام الجهاز الآخر بالـ Routing table الخاص به

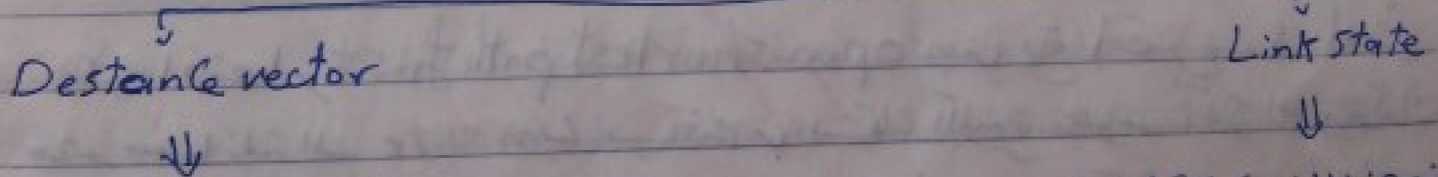


تنقسم الـ Routing protocol كما الرسم إلى نوعين :

① Interior ← داخلية [Rip، ospf، EIGRp] وهي العاملة ضمن مجال عمل واحد كالشبكات المؤسسة الواحدة أو بين المؤسسة والشركة المزودة

② Exterior ← خارجية [BGp] تصل بين مجالات عمل مختلفة ما يعرف بـ "الأنظمة المستقلة" Autonomous systems، كأنه يصل بين شركتي اتصالات مستقلتين في بلد ما أو حتى في بلدين مختلفين.

وتنقسم الـ Interior إلى



Destance vector ⇓

في هذا النوع يتم تحديد أفضل الطرق بناءً على المسافة Destance وتعني عدد الراوترات بين المنفذ وصولاً باتجاه الهدف Vector (مثال) المسار ذو الأربعة راوترات أفضل من المسار ذو الخمسة راوترات بغض النظر عن سرعة الخط بين كل نقطتين أو جهازين.
مثل بروتوكولات Rip و EIGRp

Link state ⇓

في هذا النوع يتم اعتبار حالة الـ link سرعته وكفاءته بعين الاعتبار لعدد أجهزة الراوتر التي تمر بها
مثال بروتوكولات ospf و IS.IS

مقارنة بين بروتوكولات الـ Interior

	Rip1	Rip2	Eigrp	ospf	I.S-IS
VLSM	No	yes	yes	yes	yes
Administrative distance	120	120	90	110	115
Algorithm	D.V	DV	advanced D.V	L.S	L.S
manual Summarization	No	yes	yes	yes	yes
Cisco. proprietary	No	No	yes	No	No
Max hop Count	15	15	255	No limit	

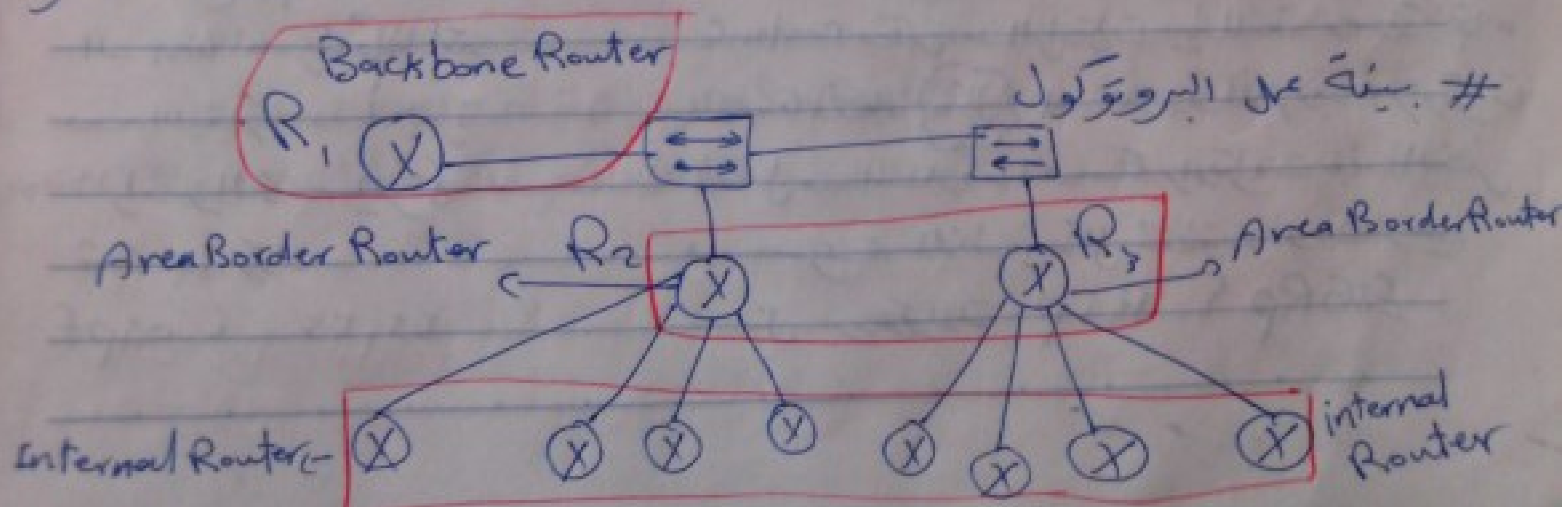
Administrative distance ← يستخدمها الراوتر في المفاضلة بين الطرق ويأخذ الأقل وإذا كان متساوي يشوف الـ cost وهو عبارة عن الـ hop count

max hop Count ← أقصى عدد ممكن أن يصل إليه البروتوكول من الراوترات.

① بروتوكول ospf

هو اختصار لـ open shortest path first يعني فتح أقصر مسار أولاً
وهو من عائلة الـ Links state يستخدم في الشبكات الكبيرة وهو من أكثر البروتوكولات استخداماً وهو بروتوكول standard أي أنه يعمل على أجهزة سيسكو وغيرها من الأجهزة

بيئة عمل البروتوكول



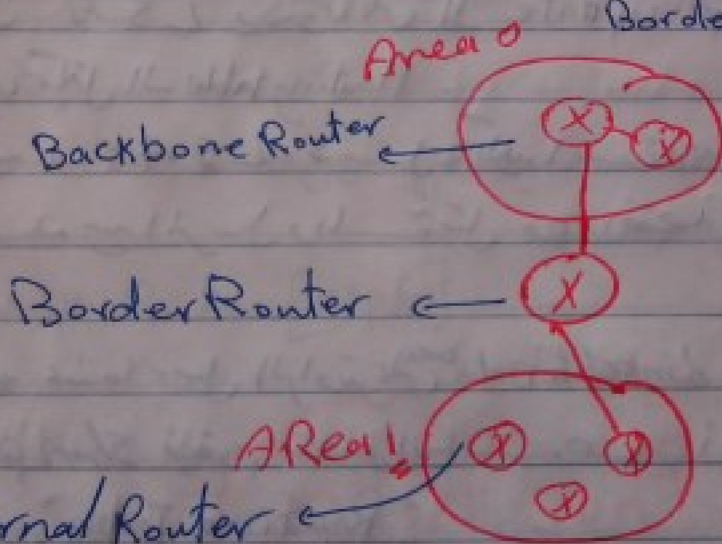
في هذا البروتوكول يتم تقسيم الشبكة إلى ٣ أقسام

① Area 0

هذه الـ Area 0 هي ما نطلق عليها Back Bone وباختصار يقسم البروتوكول الشبكات إلى مناطق المنطقة الأولى هي Area 0 وهي المنطقة التي يجب أنه يتصل بها كل المناطق الأخرى ويسمى الراوتر في هذه الـ Area بـ Backbone Router العمود الفقري.

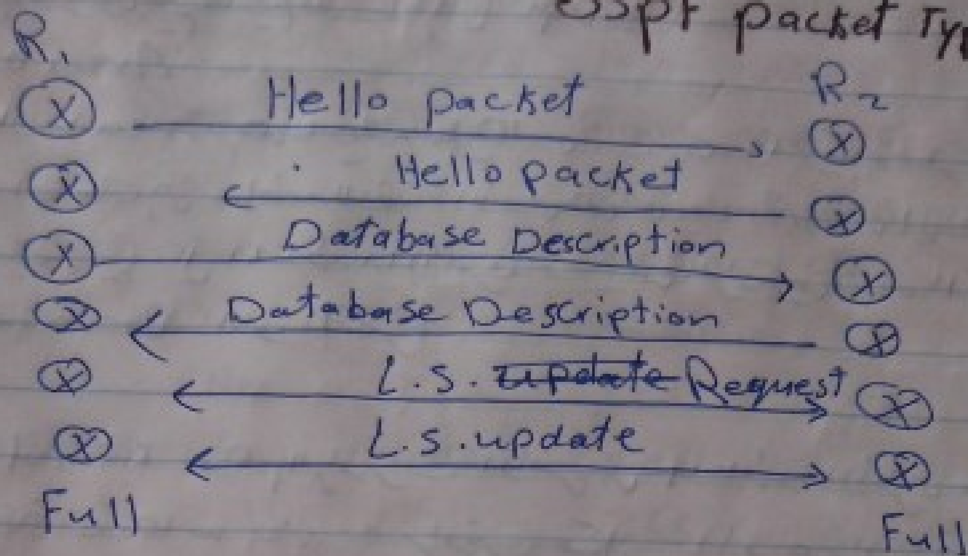
② Internal Routers وهم الراوترات الأخرى في المناطق الأخرى مع ملاحظة أنه كل منطقة عددها من ٤٠، ٥٠ راوتر فمثلا ٤٠ أو ٥٠ راوتر يشكلون Area مثل Area 1 أو Area 2 كل الأجهزة في هذه الـ Area متصلة أيضا ببعض

③ Border Router ← هي الراوترات التي تصل الأجهزة في الـ BackboneArea وهي Area 0 بالراوترات في الـ Areas المختلفة الأخرى يسمى الراوتر الذي يصل بينهم هو الـ Border Router



Hierarchical design
تقسيم هرمي أي أنه يقسم الـ Autonomous systems إلى مجموعة من الـ Area كل Area تتبادل البيانات فيما بينها

فكرة العمل } فكرة عمل البروتوكول عموما هي إرسال رسالة Hello للتعرف على الأجهزة التي تستخدم نفس البروتوكول بعد عملية التعرف كل جهاز يرسل Advertising تحتوي الراوتينج Table فيقوم كل جهاز بالمقارنة بالذي لديه هل الناقص من المعلومات. كل هذا باختصار لفكرة العمل.



يقوم كل جهاز بإرسال رسالة الـ Hello لمعرفة الأجهزة التي تستخدم البروتوكول
ثم يقوم كل جهاز بإرسال LSA تحتوي على Database الخاصة به ليقارن كل
راوتر بالـ Database الخاصة به والناقص يرسل به LSA يسد
Link state Request تطلب بيانات يريد الحصول عليها من راوتر معين فيقوم الراوتر الآخر
بإرسال LSA يحتوي على الـ update للجزء المطلوب من الجهاز الآخر
وبالتالي تكتمل الـ Routing table .
بالنسبة لـ LS Ack ترسل لتأكيد استلام أنواع الباكيت المختلفة المستقبلة
والمرسلة بين المرسل والمستقبل وهي اختصار Link state Acknowledgment

* هام * عندما يحصل الراوتر على Linkstate Database يأتي دور خوارزميات SPF
Short path Frist فيقوم بتحليل البيانات وحساب أفضل المسارات وبناء الـ Table
الخاص به "Routing Table".

OSPF Topology

بروتوكول OSPF يقوم بإنشاء ثلاث جداول كل جدول له وظيفة محددة.
وهي

① Neighbor Table
② OSPF Topology database
③ Routing Table

1. Neighbors Tables

يحتوي هذا الجدول على قائمة من جيران الراوتر ولكي يتم الحكم على الراوتر جار له أم لا لابد أن يكون مشتركين في نفس الـ Area وأن يكونوا متصلين مع بعض اتصال مباشر عن طريق Links وأن يكون لهم نفس Timers وهي الـ Hello والـ Dead

Hello ← تخبر الراوتر بجيرانه [١٠ ثواني أو ٣٠ ثانية]

Dead ← الوقت الذي إذا لم يستجب فيه الراوتر يرد فيعتبر Dead ميت ويتم إزالته من قائمة الجيران [٤٠ ثانية]

يمكن استعراض الجيران عن طريق الأمر

Router # show ip ospf neighbors

2. OSPF Topology Database

يسمى أيضاً OSPF Topology table أو [LSDB] يوضع به جميع المسارات إلى الـ Destination في الشبكة ويمكن استعراضه عن طريق الأمر التالي

Router # show Ip ospf Database

3. Routing Table

يسمى أيضاً Forwarding database ويتم فيه وضع أفضل مسار لأي Destination في الشبكة ويمكن استعراضه بالأمر التالي

show Ip Route [ospf]

OSPF Configuration

I. Single Area Configuration

① تفعيل البروتوكول وتحديد رقم العملية

Router(Config) # Router ospf 1

استدعاء البروتوكول — رقم العملية

② ادخال الشبكات باستخدام ال wildCard mask

ال wildmask هو عبارة عن قلب الوحايد إلى اصفار والعكس

المسال 255.255.255.0 تكون ال wildmask هو 0.0.0.255

مثال آخر يوضح طريقة الحساب

/28 → 255.255.255.240

255.255.255.255

---

wildmask ← 0 . 0 . 0 . 15

الأمر هو :- Router(config-Router) # Network 10.0.0.0 0.255.255.255 Area 0

← مثال

← لابد أن تكون أول Area هي 0 وتعتبر هي ال Backbone

ال Config الخاصة بال Single Area :-

Router # Config T

Router(Config) # Router ospf 1

Router(config-Router) # Network IP + wildmask Area 0

[2] Multi Area Configuration

تحقق ال multi Area هو وجود أكثر من Area وبالتالي يوجد أكثر من نوع من الراوترات وهي روترات Area 0 وهي الروترات ال Backbone ووجود روترات في Areas أخرى غير Area 0 وهي ال internal Routers والنوع الثالث روترات ABR وهي Area Border Router وهي التي تربط بين Area وأخرى.

بالنسبة لل Config لن تختلف عن Single كل ما نقوم بتفعيل ال ospf على كل راوتر في Areas المختلفة ونعرفه على الشبكات المتصلة به وعن طريق LSA سيتعرف على الشبكات الأخرى

* ملاحظة رقم العملية عند تعريف ospf لابد أن تكون ثابتة في الراوتر الواحد بمعنى أنني إذا

أردت ادخال شبكة على عملية ١٠

Router(Config) # Router ospf ١٠

وبعد إذا أردت ادخال شبكة أخرى على نفس الراوتر فإن أدخلها على نفس العملية

Router(config) # Router ospf ١٠

وبعدها أكتب الشبكة أو أي تعديل مراد ادخاله تحت هذه العملية.

Router ID

هو رقم ID خاص بالراوتر لاتشابه مع غيره من الروترات في نفس الـ Area ويتكون من ٣٢ Bit وله نفس صيغة الـ Ipv4.

عند إرسال رسالة LSA تحتوي هذه الرسالة على معلومات من ضمنها الـ RouterID

ويمكن تحديد الراوتر ID عن طريق

١- الكتابة بالأمر المباشر

(Config-if) # Router-Id <ip address>

٢- إذا لم نكتب هذا الأمر سيتم اختيار أعلى Loopback Ip address وهي عبارة عن بورت وهمي تنشئه ونعطيه Ip

٣- في حالة عدم انشاء loopback سيتم استخدام أعلى Ip موجود في physical interface في الراوتر.

⟸ باختصار RouterID

١- الأمر المباشر. وإلا

٢- أعلى Loopback Ip وإلا

٣- أعلى physical interface Ip

* يتم اختيار الـ Router ID في عملية الانتخابات لاختيار الراوتر الرئيسي

ID Configuration

الطريقة (١) Router#(config-Router) # Router-Id <ip address>

Loopback طريقة (config) # int loopback 0

(config-if) # Ip address ip mask

(config-if) # No shut

بعد اختيار الطريقة تكتب الأمر Router# clear ip ospf process
وذلك لمسح الراوتر Id الذي اختاره الراوتر سابقاً وبعد هذا الأمر سيتم استخدام
الـ Id الجديد الذي أدخلناه.

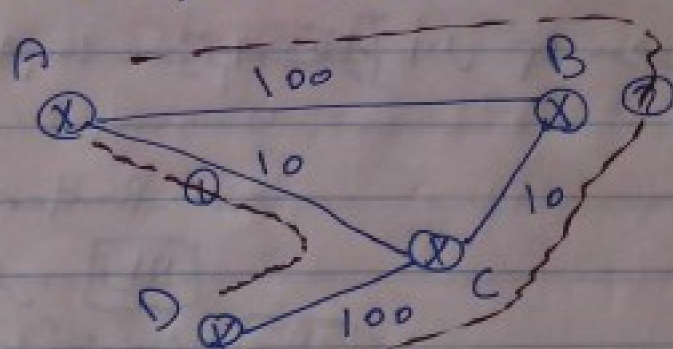
ospf metric

الـ metric هو المعيار الذي على أساسه يختار البروتوكول المسار المفضل لخروج البيانات.
يعتمد الـ ospf على الـ cost ويتم حساب الـ cost عن طريق المعادلة

$$cost = \frac{100000000}{Linkspeed}$$

حيث $100000000 = 10^8$ Bit أو 100 ميجا
و Linkspeed هو حجم الـ Bandwidth بالـ Bits أو الميجا.
فلو كان لدي Link سرعته 10 ميجا ∴ سيكون الـ cost $= \frac{100}{10} = 10$
ولو كان لدي Link سرعته 100 ميجا ∴ سيكون الـ cost $= \frac{100}{100} = 1$
والمسار صاحب اقل تكلفة هو الذي يختاره البروتوكول في الـ Routing table

مثال



نلاحظ أن الراوتر A يصل إلى الراوتر D عن طريق مسارين هو ١ و ٢

المسار رقم (1) نجد أن الـ cost الاجمالي $= \frac{100}{10} + \frac{100}{100} = 10 + 1 = 11$
المسار (2) 〃 〃 〃 $= \frac{100}{100} + \frac{100}{10} + \frac{100}{100} = 1+10+1 = 12$
∴ المسار رقم ① أفضل مسار، حيث أنه صاحب الـ cost الأقل لذلك
هذا المسار هو الذي سيوضع في الـ Routing table وأما المسار الآخر بالاضافة
للمسار ① سيوضعان في الـ Topology tables حيث أنه يوضع فيه جميع
المسارات الموصلة للـ Destination

كيفية اختيار مسار محدد

لاحظنا أن المعيار أو ال metric هو ال cost الذي يعتمد على ال Bandwidth
لذلك إذا غيرنا قيمة الباندويث نستطيع تغيير ال cost وبالتالي تغيير المسار المفضل

① تغيير ال cost مباشرة عن طريق الكتابة

(Config-if) # ip ospf Cost <no.>

② تغيير قيمة الباندويث

(Config-if) # bandwidth <no. in kbps>

③ تغيير ال Referance

نلاحظ أن الكابل ال ... ميجا التكلفة ال cost الخاص به هو 1 نلاحظ أن ال cost لا تقبل الكسور، حيث أن الكابل ال ... ميجا الجيجا تكلفته هي $\frac{100}{1000} = \frac{1}{10}$ وبما أن ال cost لا تقبل الكسور سيتم حسابه 1 وبالتالي الكابل 100 ميجا = 1000 ميجا لذلك نلجأ لزيادة ال $Referance = 10^8$ نجعله بدل 100 ميجا تكون 1000

لتكون الكابل ال 100 ميجا $= \frac{1000}{100} = 10$ والجيجا $= \frac{1000}{1000} = 1$
فيختار الجهاز المسار الذي فيه الكابل الجيجا

Router (Config-Router) # ospf auto cost Referance-bandwidth <no>

Load Balancing

لاحظنا أن ال cost يتغير من مسار لمسار، لكن بفرض أنه كان هناك أكثر من مسار لل Destination لهما نفس ال cost هنا يستطيع ال ospf أن يرسل من خلال أكثر من مسار، وهي by Default أربع مسارات وأقصى عدد مسموح به 6 مسارات

Router (config-Router) # maximum-path <no.>

OSPF Network Types

لدينا ٣ أنواع من الشبكات التي يعمل عليها الـ OSPF وهي



1 point-to-point

وهي تكون بين طرفين أي روترين وتستخدم في نقل البيانات هي PPP و HDLC
وتتصل هذه الشبكات عن طريق السيريال وهي wan Connection

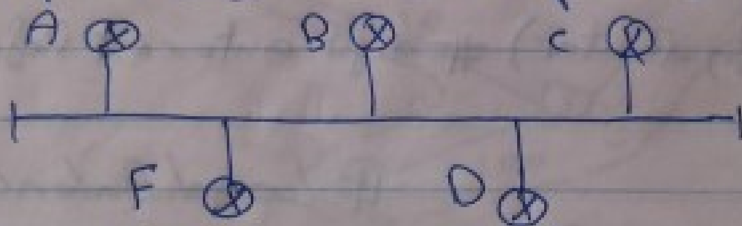
2 NON BroadCast multi Access

هي شبكات ليس لها القدرة على عمل BroadCast وتحتاج Config خاصة للتعرف على الـ neighbors في الشبكة

3 BroadCast multi Access

هي شبكة فيها أكثر من روترين تستطيع ارسال BroadCast وكذلك multiCast
يكون فيها جهاز رئيسي يسمى designated Router ويكون فيها نائب له وهو Backup designated Router يختصر الأول إلى DR والثاني إلى BDR ووظيفة الاختيار هي تقليل عملية الـ Loop وكمان ابعد الـ Loop ب

مثال



عند ارسال Hello packet من الجهاز A سيرسل إلى B و C و D و F
F . D . C . A " " B " " " " "
F . D . B . A " " C
F . C . B . A " " D
D . C . B . A " " F

فكل جهاز يرسل لكل الأجهزة تلك عند صنع ارسال LSA أو LSU فلو تم الارسال لكل الأجهزة ستحدث عملية الـ Loop

من جهاز A مثلا ارسل update لكل الأجهزة التي تستقبلها وترسلها مره أخرى لكل الأجهزة وبالتالي ستتكرر عملية ولا تنتهي عملية ارسال البيانات لذلك كان الحل في انتخاب رئيس ونائب رئيس يتم ارسال الـ LSA إليها ويقوم الرئيس بإرسال الـ LSA إلى الأجهزة الأخرى ولا يرسل للجهاز الأصلي ولا حاجة لا يرسل للـ Backup

(مثال) في المثال السابق بافتراض A هو الـ DR و B هو BDR إذا كان C يرسل LSA فانه يصل إلى A و B ويقوم A وهو الجهاز الـ (DR) بإرساله إلى F و D وبالتالي قلت عملية الـ Loop .

كيفية اختيار الـ DR و BDR

(1) يتم اختيار الـ Dr ونائبه BDr على أساس الـ interface صاحب أعلى قيمة priority أي أولوية والـ priority رقم مكون من 8Bit في عدد من صفر إلى 255 ويكون الـ default proirity (هو = 1) ويمكن التعديل فيه

Router(Config) # int F0/0 مثلا

Router (config-if) # ip ospf proirity <no>

مع ملاحظة أن الرقم لو كان صفر فهذا معناه أن الـ interface لن تكون Dr أو BDr وكذلك ليس معنا أن interface هي Dr في راوتر معين أن تكون كل البورتات في هذا الراوتر Dr بل كل شبكة مستقلة بترشيح الـ Dr من البورتات في هذه الـ Topology

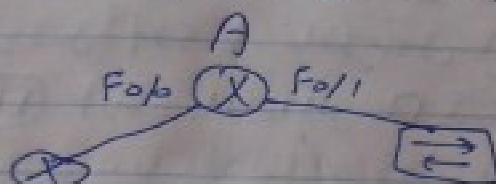
(2) إذا كانت جميع الـ proirity متساوية يتم اختيار صاحب أعلى Router ID ليكون هو الـ Dr ونائبه الذي يليه

مع ملاحظة أنه اذا تم ~~[illegible]~~ توصيل راوتر جديد صاحب proirity أعلى فإنه لن يكون الـ Dr لأنه لا يتم الانتخاب سوى مرة واحدة لكن اذا سقط الـ Dr أو تعطل وتجاوز مدة الـ Dead فإن نائبه يكون الـ Dr ويتم اختيار BDr جديد

* الروترات ترسل إلى DR و BDR على multicast address هو 224.0.0.6
* الـ DR يرسل للروترات الـ updates على multicast address هو 224.0.0.5
وده طبعًا للروترات اللي مشتركين معاه في الـ Area

الـ passive interface

بما أن في بعض الأحيان يكون متصل على البورت سويتش وآخر روتر مثل الشكل التالي



في هذا الشكل البورت Fo/1 متصل بسويتش فلا حاجة لإرسال الـ Hello packet عليه لأن ذلك سيقلل من cpu الخاص بالراوتر ولذلك في حالة إزالة السويتش وإضافة راوتر سيمنع الحصول على الـ Routing info وبالتالي فإن الـ passive int هي تعطيل المعلومات على هذه البورت فيؤدي ذلك إلى توفير حمايه أعلى وكذلك تقليل استهلاك الـ cpu

```
Router (config) # Router ospf __ _
Router (config-Router) # passive interface o/1
```

وللإلغاء نسبق الأمر السابق بكلمة No

```
No passive interface F___
```

* في هذه الخاصية "passive" تمنع الـ Hello وكذلك Advertising كل ١٠ دقيقة مستمرة.

خلاصة الـ ospf Config

① Basic ospf

```
Router (Config) # Router Ospf _1_ ex
Router(Config-Router) # Network _IP_ + _wildmask_ + Area _ex_
```

2 Router ID

مباشر Router(config-Router) # Router-id ___IP address___

Loopback Router(config) # int loopback ___0 or___

Router(config-if) # IP address ___ ___ IP mask

Router # clear IP ospf process

3 priority

Router(config) # int F0/0

Router(config-if) # ip ospf priority <no.>

4 Cost

Router(config) # int f 0/1 or

مباشر Router(config-if) # ip ospf Cost<no>

تغيير الباندويدث Router(config-if) # bandwidth <no.inKbps>

Router(Config-Router) # ospf Auto-Referance bandwidth <no.>

5 cost تحديد المسارات في حالة تساوي ال

Router(Config-Router) # maximum-path <no.>

6 ضبط التوقيتات

(config-if) # ip ospf hello-interval <no.in sec>

(config-if) # ip ospf Dead-interval <no.in.sec>

7 Show Commands

show ip protocols — عرض البروتوكولات المستخدمة

show ip Route ospf — عرض المسارات الخاصة بـ ospf

show ip ospf interface — عرض البورتات الداخلة في ospf

show ip ospf — معلومات عن LSA { Timers , Id

show ip ospf neighbors — الجيران

show ip ospf process — العمليات

show ip ospf data base — الداتا بيس للراوتر

لمسح ال Routing table

Router# clear IP Route

EIGRp protocol

بروتوكول EIGRp هو اختصار لبروتوكول Enhanced Interior Getway Routing protocol وتعني بروتوكول البوابة الداخلية المحسنة وهو بروتوكول خاص بأجهزة سيسكو Cisco proprietary وهو النسخة المحسنة من بروتوكول Interior getway Routing protocol IGRp وهو بروتوكول Distance vector

ميزاته

١- سهولة الإعداد حيث أنه لا تتطلب خبرة كبيرة
٢- البروتوكول الوحيد الذي عليك مسار احتياطي حيث تمكنه الحصول على مسار احتياطي في Topology إذا فقد المسار الأساسي.
٣- الـ Summarization مفعل عليه تلقائياً ويمكن ايقافه عن طريق no Auto-Sammary
٤- يعتبر أكثر البروتوكولات استخداماً في عملية الـ Routing
٥- بروتوكول hybrid يجمع بين سهولة الـ Distance vector وقوة الـ Links stat

عيوبه

١- يعمل مع أجهزة سيسكو فقط
٢- بعض التعقيد في حساب الـ metric

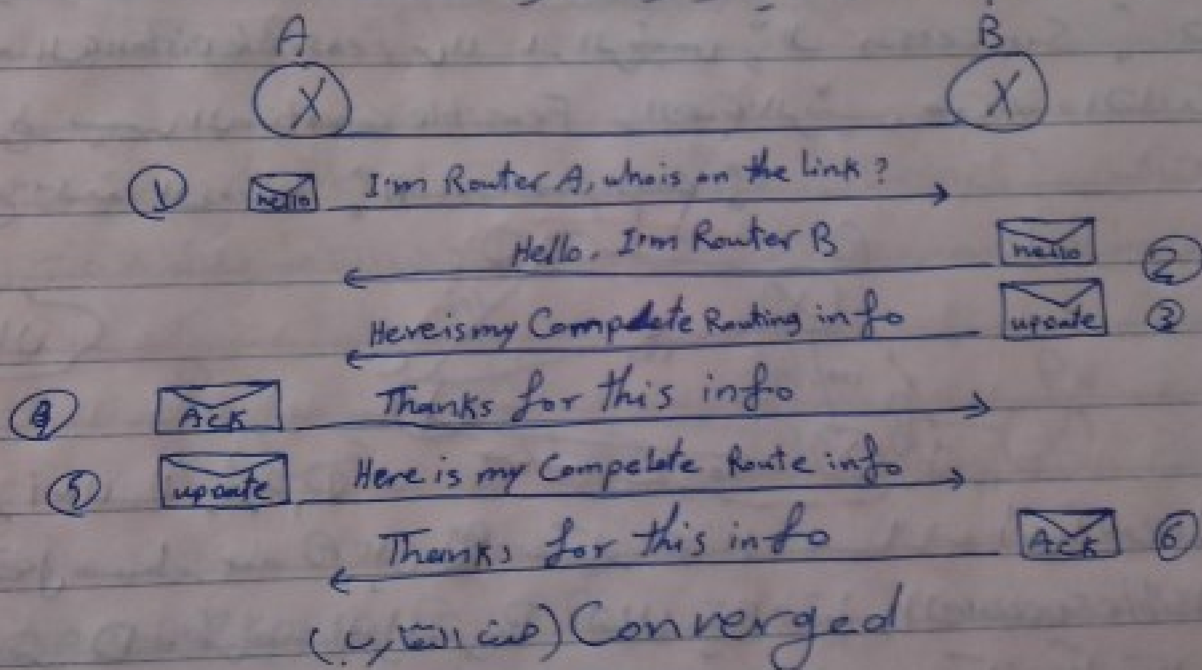
جداول EIGRp

بروتوكول Eigrp يقوم أيضاً بإنشاء ٣ جداول
① Neighbor Table ؛ ويحتوي على معلومات جميع الجيران في الشبكة ويظهر بالأمر
#show ip eigrp neighbor
② Topology Table ؛ يستخدم لمعرفة أفضل مسار Successor وثاني أفضل مسار Fisable Successor ويظهر بالأمر #show ip eigrp Topology
③ Routing Table ؛ لمعرفة أفضل مسار في عملية الـ Routing ويظهر بالأمر # show ip Route

إنشاء العلاقات مع الجيران

يستخدم بروتوكول الـ Eigrp ٥ رسائل لإنشاء العلاقات مع جيرانه وكذلك أيضاً للتنبيه بحصول الأخطاء حتى يقوم باستخدام الروابط الاحتياطية Fisable seccessor
يقوم الراوتر بإرسالها. "رسائل الـ Eigrp" في صورة multiCast من واحد إلى مجموعة
وتفاصيل الرسائل بالرسم التوضيحي الشكل التالي

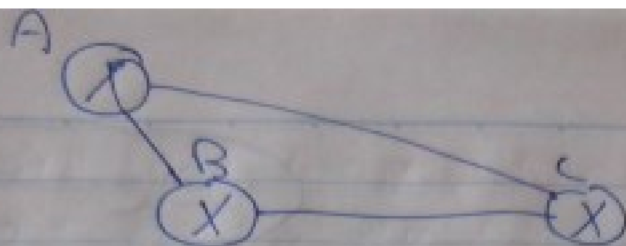
1. Hello packet ⇐ للتعرف على الروترات الأخرى
2. upDate packet ⇐ لإرسال معلومات وتحديثات الـ Routers
3. Query packet ⇐ للاستعلام عن المسارات الأخرى عند فقدانه المسار الأصلي
4. Replay packet ⇐ الاستجابة لـ Query المرسلة وإعلام المرسل بالمسار الاحتياطي
5. Ack packet ⇐ تأكيد وصول المعلومات.



Converged (حدث التقارب)

بعد تشكيل العلاقات بين الراوترات يأتي تحديد المسارات الرئيسية والمسارات الاحتياطية أو ما تعرف بـ Successor و Fisable successor.
ويتم تمييز هذه المسارات عن طريق حساب الـ Advertised Distance و Feasable Distance

1. Advertised Distance ⇐ هي المسافة بين الراوتر المجاور وبين الوجهه النهائية
2. Feasible Distance ⇐ هي المسافة الكلية بيني وبين الوجهه النهائية بما فيها ذلك الـ AD أي المسافة بين الراوتر الجار والوجهة النهائية.



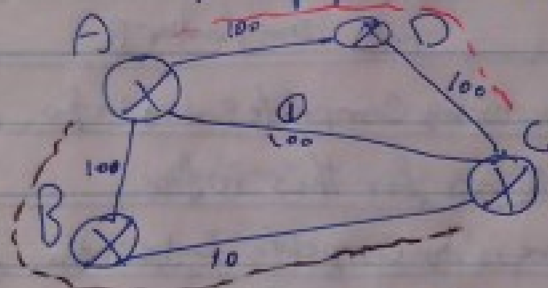
مثال

اذا كان A يقصد الوصول إلى C فإن أفضل مسار هو الرئيسي Successor والثاني يسمى Feasible successor وبالنسبة لل Advertised Distance هي المسافة من الجار للوجهة النهائية وهي هنا من B إلى C بينما ال Feasible distance هي المسافة الكلية إلى C = المسافة من A إلى B + المسافة من B إلى C

تحديد ال Successor و Feasible Successor

ال Successor ← هو المسار صاحب أقل تكلفة

ال Feasible successor ← هو المسار الاحتياطي صاحب ثاني أقل تكلفة لكن هنالك شرط حتى يكون Feasible suc. وهو أن تكون ال Advertised Distance في هذا المسار أقل من ال Feasible Distance في المسار الرئيسي "ال Successor" هذا الشرط يسمى ال Feasible condition والهدف الرئيسي من هذه القاعدة هو منع عملية الدوران "Loop prevention"



مثال

باعتبار أن المسار رقم 1 هو أفضل مسار من A إلى C سيكون هنالك مساران أيضاً للوصول عن طريق الراوتر D وطريق الراوتر B لذلك يتم اختيار ال Feasible successor من خلال المسار الذي فيه Advertised Distance أقل من التكلفة الكلية للمسار 1 فبفرضنا أن Ad في المسار B هي 10 و Ad في المسار D هي 100 فالمسار الذي فيه Ad أقل من التكلفة الكلية للمسار الرئيسي هو B ← المسار B هو Feasible successor

EIGRP Metric

ال metric الخاص بهذا البروتوكول معقد نوعاً ما فهو يعتمد على خمس قيم وهي Bandwidth (K1) و Delay (K3) و Relibility (K4 & K5) و Loading

وحيث اعتبار K_1 و $K_3 = 1$

K_2 و K_4 و $K_5 = 0$

فيكون الـ metric بالوضع التالي

$$metric = 256 \times (Bandwidth + Delay)$$

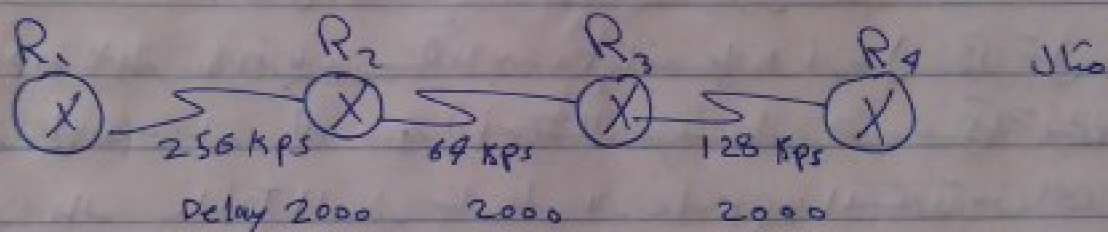
① الباندويث " Bandwidth " وهي عبارة عن أقل سرعة موجودة بين الـ source والـ Destination

$$Bandwidth = \frac{10^7}{least\ bandwidth\ in\ kps}$$

وهو يساوي $\frac{10^7}{\text{أقل باندويث في الكابلات الواصلة للوجهة النهائية}}$

② التأخير " Delay " وهو عبارة عن مقدار التأخير الذي يحصل في الوصول بين الـ المصدر والوجهة النهائية " إجمالي التأخير في الكابلات "

مثال



نلاحظ أن سرعة الكابل بين الراوترين R_2 و R_3 هو 64 kps وهو صاحب أقل Bandwidth لذلك هو الذي سيدخل في الحساب في حين أن الـ Delay لا يختلف فنأخذ القيمة 2000 مع أنها ثابتة في كل الكابلات.

$$metric = 256 \left(\frac{10^7}{64\,kps} + 2000 + 2000 + 2000 \right)$$

$$metric = 256 \times (156250 + 2000 + 2000 + 2000)$$

$$metric = 256 \times (156250 + 6000)$$

$$metric = 256 \times 162250$$

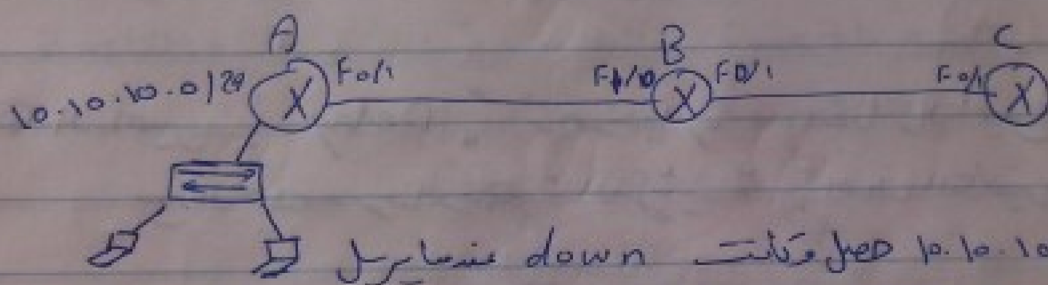
$$\boxed{metric = 41536000}$$

بعد حساب الـ metric يتم تحديد الـ Successor وكذلك الـ Feasible successor
مع مراعاة أن تكون الـ Advertised D. في المسار الاحتياطي لا تزيد ولا تساوي
المسار الرئيسي.

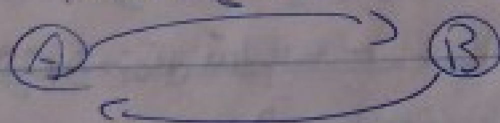
* يستخدم بروتوكول Eigrp خوارزمية تسمى Dual وهي اختصار
لـ Diffusing update Algorithm وهي المسئولة عن اختيار المسار الرئيسي والاحتياطي
حيث أنها تستعلم كل المسارات من الراوترات الجار، وكذلك المسئولة عن استخدام المسار الاحتياطي في
حالة تعطل المسار الرئيسي

مشكلة الـ Routing Loops

شرح



بفرض أن الشبكة 10.10.10.0 حصل وكانت down عندما يرسل
A الـ update للروترات الأخرى يرسلها بعد 30 ثانية فإذا أرسل B قبل أن
يرسل A الـ update فإن A سيقرأ أن هناك مسار جديد لشبكة تسمى 10.10.10.0
وبالتالي يسجل في الـ Table المسار بناء على الـ update المستلمة من الجهاز B
ثم يرسل A الـ update لـ B فيجد أن هناك شبكة 10.10.10.0 مسارها عند
A فيسجلها ثم يرسل B update وهكذا تحدث عملية دوران



هذه العملية تسمى Routing Loop ويمكن التخلص من هذه العملية
عن طريق ① max hop count
② Split Horizon
③ Route poisoning
④ Holddown timers
⑤ Triggered update

① max hop count

هذه الخاصية تجعل عملية الـ Loop تحدث فقط ١٦ مرة أي أن عملية الدوران بين الراوترات



تحدث ١٦ مرة فإذا وصلت ١٦ مرة ولم يصل الراوتر للشبكة يعتبر الشبكة down ولا وجود لها.

② split Horizon

هي خاصية تمنع ارسال المعلومة إلى مصدر المعلومة بمعنى آخر لو A أرسل إلى B وجود أن شبكة متصلة بـ A وقعت لا يقوم B بإرسال update لـ A ليبلغه مسار الشبكة حيث أن الاصل A هو الذي علم B عنها وبالتالي لا يحدث الـ Loop وبالتالي طالما يرسل A الـ update المحتوي على معلومة أن الشبكة Down يجعلها B عنده down. وهكذا

③ Route poisoning

تسمم المسار وهو باختصار إذا الراوتر وجد أن هناك شبكة معينة أصبحت غير موجودة يقوم بعمل Route poisoning أي يعتبر الشبكة هذه على بعد ١٦ راوتر أو مسار وذكرنا أن ١٦ next hops أقصاها فبالتالي يعتبر الشبكة غير موجودة بدلاً من انتظار دوران الـ update بين الراوترات ١٦ مرة لا يعرفوا أن الشبكة على بعد ١٦ مسار فيجعلوها غير موجودة.

④ Triggered upoate

هي خطوة يقوم بها الراوتر بإرسال update مباشرة في حالة أن شبكة تكون down ليعلم جيرانه بها دون الانتظار للـ interval time كي لا يحدث Loop

⑤ Hold down timers

معناه لو فيه مسار فقده الراوتر فإنه لا يعتبره مفقود مباشرة بل ينتظر فترة زمنية ثم ينتظر آخر update وصله لو كان ما زال مفقود يجعله أنه غير موجود لكن لو وجد المسار يجعل أنه موجود.

خاصية Load Balancing

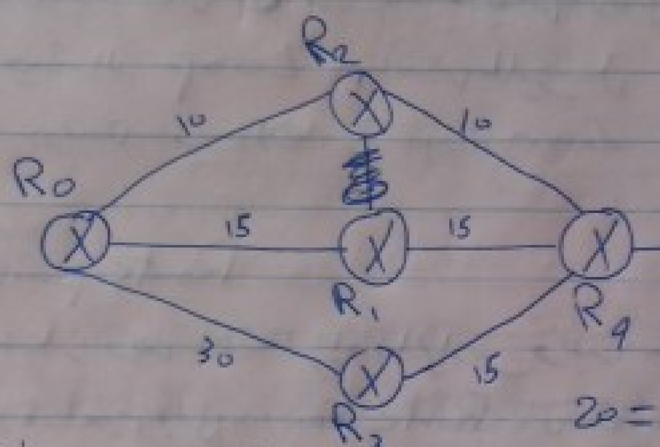
load Balancing ← هو قدرة الراوتر على توزيع الـ Traffic إلى كل الجهات والمسارات التي تكفي الوصول إلى Destination والفائدة من ذلك هي رفع مستوى الاستفادة من أجزاء الشبكة إلى أعلى استفادة ممكنة

وينقسم الـ load Balancing قسمين

Equal
يستخدم عندما تكون المسارات لها نفس الـ cost

unequal
المسارات فيه غير متساوية
ويستخدم في بروتوكول Eigrp

unequal path
مثال



كما نلاحظ أن المسار $R_0 \to R_2 - R_4 - pc$ هو أفضل مسار من R_0 إلى pc حيث الـ cost = 20
والمسار $R_0 \to R_1 \to R_4 - pc$ هو المسار الاحتياطي حيث هو صاحب أقل metric بعد المسار الرئيسي.

تكمن الاستفادة من المسارات غير متساوية في نقل الـ Traffic إلى الـ Destination عن طريق تعديل الـ Varian ce ففي الأصل = 1 فتكون الـ metric
= 20 X 1 = 20 (المسار الرئيسي) والاحتياطي هو 30 بفرض أننا غيرنا الـ varin ce لتكون 2 فتكون المسار الرئيسي = 20 X 2 = 40
أي تسمح لمن تكلفته أقل أو تساوي 40 بالمشاركة في الـ Load Balancing
وبالتالي المسار الاحتياطي = 30 وهو أقل من 40 فبالتالي يشارك في Load Balancing
بالرغم أنه لا يملك نفس metric المسار الرئيسي.

EIGRP Configuration //

Router(config) # Router Eigrp <رقم AS>

Router(config-Router) # network ip ____ . ____ wildmask

Router(config-Router) # no Auto-Summary

أوامر ال show

Router # show ip Route

Router # show ip Route eigrp

Router # show ip eigrp neighbors

Router # show ip eigrp Topology

ال varince ~~passive~~

Router(config) # Router eigrp ___ رقم

Router(config-router) # variance ___ رقم

ال passive

Router(config-Router) # passive-interface F0/0

ال maximum

Router(config-Router) # maximum path ___ (رقم)

التوقيتات

Router(config) # F 0/1

Router(config-if) # ip hello-internal eigrp ___

Router(config-if) # ip hold-internal eigrp ___

لابد يكون ال Hold ٣ أضعاف ال Hello فإذا غيرنا ال Hello نغير لازم ال Hold

بمقدار ٣ أضعاف ال Hello

Router # clear Ip Route

Administrative distance | AD

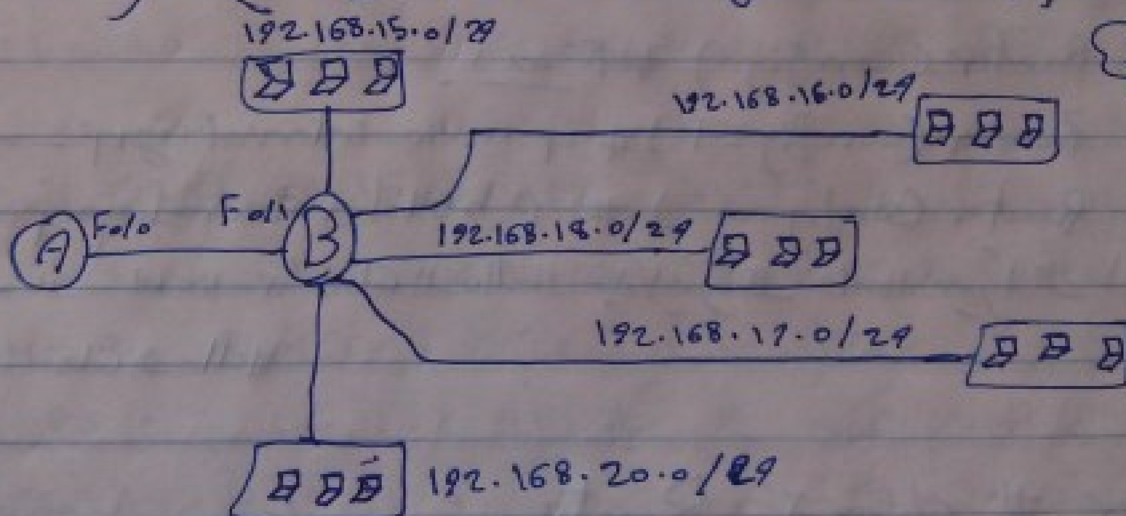
يستخدمها الراوتر في المفاضلة بين أنظمة الراوتنج بمعنى أنه لو كان شبكة تم تعريفها static وأيضا Dynamic يستخدم الراوتر ال AD لحساب ماهو النظام الذي يستخدمه وكذلك أيضا لو ال Dynamic مرة ospf ومرة Eigrp أو أي بروتوكول آخر من بروتوكولات ال Dynamic Route يستخدم الراوتر ال AD ويختار أقل رقم

Route Type	Admin Distance
Connected	0
Static	1
Eigrp	90
ospf	110

Summarization

ال Supernetting أو مايعرف ب Summarization هو عملية تجميع الشبكات إلى الشبكة الأصل وهي عكس عملية ال Cidr Subnetting

مثال



نلاحظ وجود ٥ شبكات من class C متصلة براوتر B هذه الشبكات Connected على الراوتر لكن بالنسبة للراوتر A إذا أردنا تفعيل الراوتنج Static فإننا نقوم بتعريف الشبكات شبكة شبكة للراوتر حتى يتم ادراجهم في ال Routing Table فكرة ال Summarization هي اختصار كل الشبكات وكتابة الشبكة الأم التي تجمعهم

وبالتالي لا نستخدم أن تحمل امكانيات الراوتر ولا تأخذ حيز كبير من الـ RoutingTable

لكي نقوم بإرسال تلك الشبكة نستخدم Summarization نتبع الآتي

نقوم بوضع الأيبهات تحت بعضها

192.168.15.0

192.168.16.0

192.168.17.0

192.168.18.0

192.168.20.0

الماسك لجميع الشبكات هو 24 ونلاحظ أن الاشتراك الأوكتت الأول والثاني

نستطيع الثابت 192.168 والمختلف هو الأوكتت الثالث نقوم بتحويله

إلى Binary ونأخذ الثابت والمختلف نعتبره أصفار

15 → 00001111

16 → 00010000

17 → 00010001

18 → 00010010

20 → 00010100

---

000 00000

نقوم بتنزيل الثابت والمختلف نعتبره أصفار ∴ الأوكتت الثالث = صفر

∴ الـ Cidr هو 192.168.0.0 والماسك هو 16

∴ بعد الـ Summarization هو 192.168.0.0/19

مثال آخر: الشبكة هي 207.21.54.0 والشبكة 207.21.55.0/24 نستطيع أن نجمعهم كالتالي:

الثابت

207.21.00110110.0

207.21.00110111.0

207.21.54.0/23

مثال آخر: الشبكة 200.199.98.32/27 ، 200.199.98.64/27 ، 200.199.98.96/27

نعمل لهم Summarization كالتالي

الجزء الثابت هو 200.199.98 ، اذن الأوكتت الرابع هو المختلف

نحوله لـ Binary

32 = 0 0100000

64 = 0 1000000

96 = 0 1100000

---

0 000000

∴ الأوكتت الرابع هو صفر ولكن الماسك يزيد عدد الوحايد بمقدار الثابت وهو 1 حيث أن عدد البتات الثابت في الأوكتت للثلاث أرقام هو البت الأول فقط ∴ الـ cidr هو 200.199.98.0/25

مثال آخر: الشبكات 200.199.48.0/25 ، 200.199.49.0/25 ، 200.199.56.0/23

نعمل لهم Summarization كالتالي

الـ octet الثابت هو 200.199 والـ octet المختلف هو الثالث

فنحوله لـ Binary

48 = 0011 0000

49 = 0011 0001

56 = 0011 1001

0011 0000

بالتالي العنوان هو 200.199.48.0 والماسك هو 20

فيكون الـ cidr هو 200.199.48.0/20

ACL
Access Control List

هي وظيفة للتحكم بنقل البيانات على الشبكة تقوم على أساس الفلترة Filtering وذلك بحجب البيانات الغير مرغوب فيها والسماح بالبيانات المرغوب بها أو باختصار هي مجموعة من إجراءات السماح أو المنع يتم تطبيقها على الشبكة بغرض التحكم في الشبكة.

مثال :- منع شبكة بالدخول على الانترنت في حين السماح لجهاز واحد من هذه الشبكة باستخدام الانترنت.

خصائصها :-

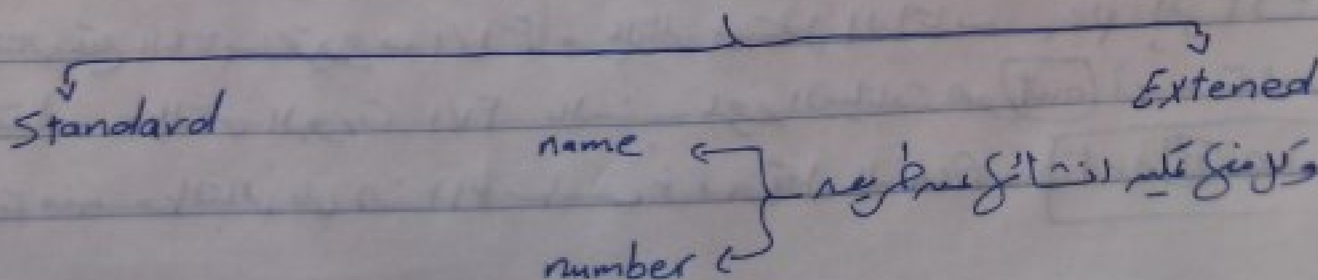
(١) هي عبارة عن مجموعة من الاوامر أو الجمل التي تساعد على التحكم في الشبكة

(٢) هذه الجمل يتم فحصها بطريقة تسلسلية مرتبة مثال على ذلك لو أردنا أن نمنع الجهاز (أ) من الاتصال بالانترنت وهذا الجهاز ضمن الشبكة رقم (٥) فإن الاوامر هي ① منع الجهاز ثم ② السماح للشبكة (٥) وبالتالي الراوتر يفهم أن المراد هو منع الجهاز ؟ والسماح لباقي الشبكة (٥) لكن إذا كتبنا السماح للشبكة (٥) أول أمر فإن الراوتر يسمح لها ثم يجد أن هناك بعدها منع للجهاز (؟) فلا يفهم حيث أنه تبع (٥) التي هناك أمر بالسماح لها بالدخول على الانترنت وبالتالي التسلسل والترتيب أمر مهم

(٣) الاوامر الضمنية :- هناك أمر ضمني لا يظهر لي ولا أكتبه لكن يتم تطبيقه بمجرد انشاء قائمة ACL يعني أنني إذا منعت الجهاز (؟) مثلاً وعامل الجهاز (ب) الاتصال بالانترنت فإنه لن يستطيع بالرغم من أنه (؟) هو الذي عليه الامر ذلك لأن هناك أمر ضمني هو "منع الكل" ينشأ بمجرد اضافة Acl على الراوتر وبالتالي نحتاج للسماح لباقي الاجهزة.

(٤) الـ Acls تكتب وتنشأ في Global mode ويتم تفعيلها على الانترفيس المراد تطبيقها عليه

أنواع الـ Access List



Standard Acls 1

هذا النوع يستخدم لعمل اجراء على Source Ip فقط سواء هذا الاجراء كان به permit أو كان deny

* (٢) طريقة الـ Name

١- في هذه الطريقة يتم كتابة اسم لـ Acls وتحديد نوعها standard

Router (config) # ip Access-list standard < الاسم >

٢- انشاء قائمة الاوامر سواء permit أو deny

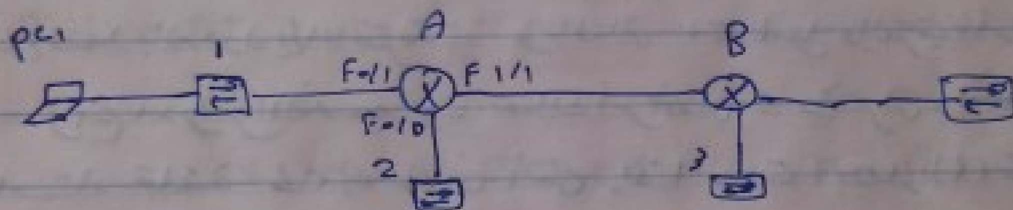
Router (config-std-nacl) # deny 192.168.10.1 + wildcard

Router (config-std-nacl) # permit any

٣- تفعيلها على الانترفيس

لابد أن تفهم ما هو الهدف من الـ Accesslist وبالتالي على أساس ذلك نستطيع تحديد البورت وهل الـ Accesslist out أو in للراوتر. وهذا يشمل كل أنواع Accesslist

(مثال)



نفرض أن الجهاز (pc1) نريد منعه عن الشبكات ٢ و ٣ وكل الشبكات المتاحة فبالتالي مسار البيانات هي الدخول بداخل الراوتر A عبر البورت F0/1 وبالتالي لو طبقنا الـ Acl عليه سيمنع الداتا من الخروج للشبكات هذا المخرج هو بالنسبة للراوتر هو الذي تدخل منه عليه البيانات من الجهاز pc1 اذن هنا نحدد البورت الذي يتم تفعيل البيانات عليه أنه (in) في نفس المثال لو أردنا أن يرسل الجهاز pc1 لشبكة ٢ ولا يرسل إلى ٣ بالتالي مسار البيانات هو pc1 ← F0/1 ← F1/1 وبالتالي نمنع الداتا من الخروج من F1/1 وبالتالي ستصل الداتا من pc1 إلى الشبكة (٢) فقط وبالتالي البورت F1/1 بالنسبة لمرور البيانات هو (out) أي ستغادر البورت منه وبالتالي على هذا الاساس نحدد ونفعل الـ Acls

in (or) out

فيكون الأمر كالتالي

Router(config-if) # ip Access-group <الاسم المختار> out / in

على حسب المسار.

فيكون اجمالي الاوامر هو:

```
Router (config) # ip Access-List standard < name >
Router (config) # permit host ____ ____ ____..
Router(config-std-nAcl) # deny __ip__ __ + wildCard          (لو شبكة)
Router(config-std-nacl) # permit any
Router(config-std-nacl) # exit
Router(config) # int Fa0/1
Router(config-if) # ip Access-group (name) + out / in
```

ملاحظة: named ACLs هي أنه لها أرقام من [1 : 199] هي أرقام الـ standard

وبالتالي لو أردنا أن نعمل تعديل في أمر ما. نتبع الآتي

① أمر الـ show لعرض رقم الأمر

Show Access-list

سيظهر بها الاجراءات التي تم تفعيلها ولكن أمر الـ permit هو 20 وأمر الـ deny كان 50 فإذا كنت محتاج أضيف أمر بينهم أكتب أرقام الأوامر السابقة عن طريق أمر الـ show

② ← كتابة الأمر الجديد بعد اضافة الرقم المناسب عن طريق الأمر

```
Router (config) # ip Access-list standard <نفس الاسم السابق>
Router (config-std-nacl) # رقم + permit / deny ______
```

ونحدد الرقم حسب المراد ترتيبه عليه لو أردناه بعد أول أمر نكتب رقم بعد رقم أول أمر وهكذا ____

③ طريقة الرقم وهي الطريقة الاشهر.

نقوم بتحديد رقم لـ Acls ويكون من [1 : 99] أو من [1300 : 1999]

وهذه الارقام خاصة بـ standard Acls

ويختلف أمر الانشاء في انشاء الـ Acls فقط بـ ip كالآتي Named كالتالي

① انشاء الـ Acls

Router(config)# Access-list + رقم + deny/permit + host + ip source

(or)

Router(config)# Access list + رقم + deny/permit + source ip + 0.0.0.0

Router(config)# Access-list + رقم + permit any

② تفعيل الـ Acls على الانترفيس

Router(config-if)# ip Access-group + الرقم + in/out

(هام) ملاحظة لو أردنا أن نسمح جهاز واحد وليكن 18.0.2.3/23 فإننا نكتب الأمر

Router(config)# Access-list + رقم + permit + ip source + subnet mask

فهذا نسمح لجهاز واحد (كله) اذا كنا كتبنا الـ IP الخاص بـ source

وكتبنا الـ wildmask فاننا نسمح لـ شبكة كلها حتى لو كتبنا عنوان ip واحد فقط.

Standard Config

① جهاز واحد.

Router(config)# Access_list + رقم + permit/deny + host + ip source / 0.0.0.0

Router(config)# Access list + رقم + permit/deny + ip source

② سمح/منع شبكة كاملة

Router(config)# Access-list + رقم + permit/deny + ip الشبكة + wildmask

③ تفعيل الـ Acls على الانترفيس

Router(config-if)# ip Access-group + الرقم + in/out

Router# Show Access_list

Extended Access-list [2]

هذا النوع يستخدم في تقييد البكات packet العديد من الأمور مثل Source IP وكذلك Destination Ip وكذلك نوع البروتوكول وكذلك رقم البورت وبالتالي هذا النوع يتيح لنا تحكم خواص في التحكم في الشبكة أكثر من النوع الـ standard

(أ) طريقة الـ Name

```
Router(config)# ip Access-list extended + < الاسم >
Router(config-ext-nacl)# permit + البروتوكول + host ipsource host Destination eq + البورت
```

مثال

```
Router(config-ext-nacl)#permit Tcp host 18.0.2.3 host 18.0.0.4 eq 69
Router(config-ext-nacl)# deny icmp host___ host____
Router(config-ext-nacl)#permit icmp any any
```

مثال آخر

* تفعيلها على البورت بعد تحديد المسار out أو in على الراوتر

```
Router(config-if)# ip access-group < الاسم > + in / out
```

(ب) طريقة الـ number

الـ extended الأرقام الخاصة بها تكون إما من (100 : 199) أو من (2000 : 2699)

* الاستثناء.

```
Router(config)# Access-list 110 deny TCP host _IP_ + host _IP_ eq _رقم البورت_
Router(config)# Access-list 110 permit Tcp any any
```

* التفعيل على البورت

```
Router(config-if)# Ip Access-group in
```

و الصفحة التالية فيها الـ Configuration الخاصة بـ Access-list بصورة أوضح

① منع جهاز بجهاز

Router(config)# Access-list 101 deny ip host __IP__ host __IP__

Router(Config# Access-list 101 permit ip any any

② منع جهاز من التواصل مع شبكة

Router(config)#Access-list 102 deny ip host __IP__ + __Network__ + __wildCard__

Router(config)# Access-list 102 permit Ip any any

③ منع شبكة من شبكة.

Router(config)# Access-list 103 deny Ip __Network__ + __wildcard__ + __Network__ + __wildCard__

Router(Config)# Access-list 103 permit any any.

④ منع شبكة من التواصل مع جهاز

Router(Config)# Access-list 104 deny ip __Network__ + __wildcard__ + host __IP__

Router(Config)# Access-list 104 permit ip any any

⑤ إعدادات الـ Telnet

١- أولاً نفعل خاصية الـ Remote Access بالطريقة العادية.

٢- نكتب الأوامر على الـ global mode

Router(config)# Access List + رقم + deny/permit + host __IP Source__

أو

Router(config)# Access-list + رقم + deny/permit + __IP Source__ + 0.0.0.0

③ نعرف الإعدادات على الـ VTY

Router(Config)# line VTy 0 4

Router(config-line)# Access-class + نفس الرقم + in/out

وللإلغاء

Router(Config)# No Access List + الرقم +

أوامر الـ show الخاصة بـ Access-List

R # show access-list → . يعرض كل الـ Access-list
R# show access-list 110 → . يعرض الـ Access التي رقمها ١١٠
R#show Ip interfaces → . يعرض كل شيء على الانترفيس
R#show Running-Config → . يعرض كل شيء

* تقبل التعديل على الـ Named Access-List ولا تقبل التعديل على numbered Access-List
فلم نلغي الـ Access-List ونعيد كتابتها.

DHCP

هو اختصار Dynamic host Configuration protocol ويعني بالعربية بروتوكول التشكيل الديناميكي
وهو بروتوكول يقوم بإعطاء عناوين (Ips) للأجهزة الشبكة بصورة أوتوماتيكية بدلاً من الطريقة
اليدوية.

س: كيف يعمل DHCP ؟
هناك ٤ خطوات لكي يحصل أي جهاز على عنوانه من خلال DHCP

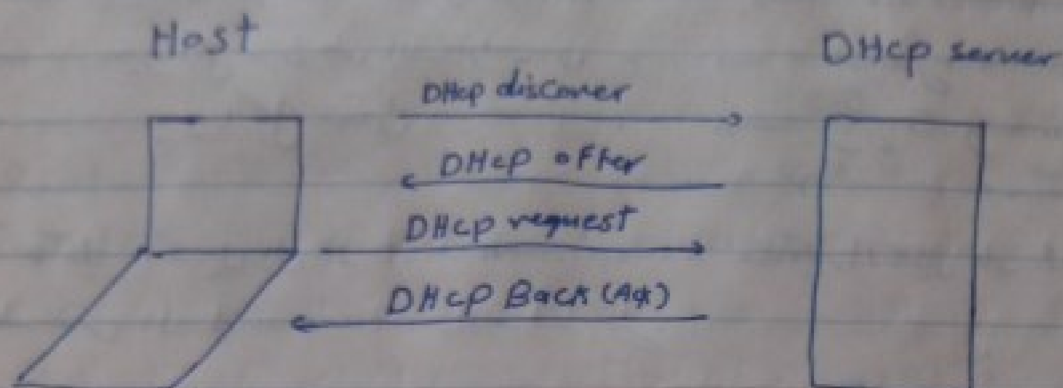
1 DHCP discover :
يقوم الـ Host في هذه الخطوة بإرسال رسالة على شكل Broad Cast فيرسلها إلى
255.255.255.255 في حين أنه حتى الآن لا يملك عنوان فيكون عنوانه في هذه الخطوة هو 0.0.0.0
أي 0.0.0.0 يرسل إلى 255.255.255.255 رسالة تتضمن الـ macaddress

2 DHCP offer :
عندما تصل رسالة الـ Host للعنوان 255.255.255.255 فإنها تصل لكل الأجهزة في الشبكة ومن ضمنها
سيرفر الـ DHCP الذي يرد عليها بعرض خدماته من خلال حزمة DHCP offer وفيها يقترح على
الجهاز الطالب عنوان Ip مع باقي المعلومات الملحقة به ويتم حجز هذا العنوان بشكل مؤقت لحين ورود
تأكيد بقبوله من الجهاز الـ Host

3 DHCP request حيث يقوم الـ Host بالرد على السيرفر بإرسال حزمة DHCP request تعلمه بنيته
استخدام العنوان المقترح

④ DHcp Back :

وتسمى أيضا Acknowledgment وفيها يرسل السيرفر الـ Host التأكيد وإتمام عملية التأجير.



بالنسبة إلى اعداد سيرفر DHcp فإننا نقوم بالآتي:

* تحديد مجال [بداية ونهاية] العناوين التي سيتم تأجيرها للأجهزة و Subnetmask
* تحديد العناوين التي سيتم استثنائها من عملية التأجير والتي على الاغلب ستكون محجوزة لاستعمالات الأجهزة الثابتة التي لا مجال لتغيير عناوينها كالسيرفرات.
* مدة التأجير وقد تتراوح من عدة دقائق إلى ساعات وأيام أو حتى إلى الأبد
* عنوان الـ Default getway
* عنوان سيرفر الـ DNS

DHcp Configuration

① إنشاء DHcp address pool وإعطاء اسم لها.

Router(config) # ip dhcp pool ____Name____

② تحديد العناوين التي سيتم توزيعها في الشبكة:

Router(dhcp-Config) # network ________ + mask

③ تحديد الـ Default getway

Router(dhcp-Config) # default-Router + ____IP getway____

④ تحديد الـ DNS

Router(dhcp-Config) # dns-server ____ex____.

⑤ في حالة استثناء بعض الايبهات

Router(config) # ip DHcp excluded address _IP_ + _IP_

(إلى + من)

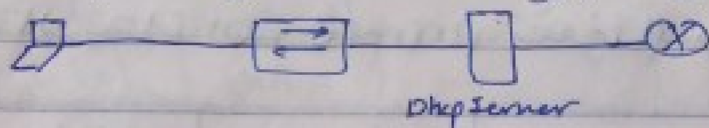
⑥ تحديد وقت الـ lease الايجار

Router(dhcp-config) # lease 1 5 20 مثال

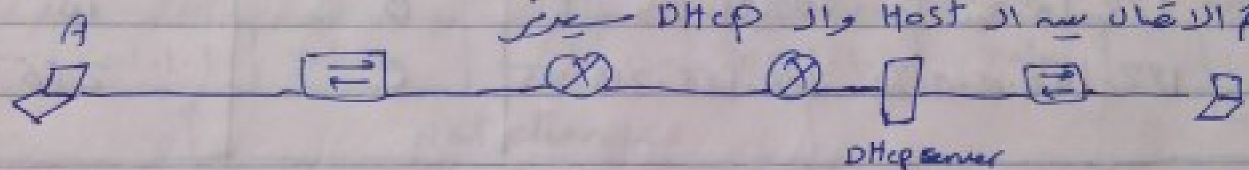
يوم ← ساعة ← دقيقة ←

* لو السيرفر DHcp في شبكة أخرى *

ابتداء عندما يقوم الـ Host بإرسال رسائل الـ Discover فإنه يرسلها كما وضحنا على هيئة Broadcast فتصل لكل الأجهزة المتصلة في نفس الشبكة.



لكن إذا كان السيرفر في شبكة ثانية تفصل بينهم أجهزة الراوتر فإن رسائل الـ Broadcast لا تمر من الراوتر لانه ترسل للشبكة التي فيها فقط وبالتالي لن يتم الاتصال بين الـ Host والـ DHcp سيرفر



و لكي نحل هذه المشكلة نفعل أمر يتيح لنا الحصول على DHcp سيرفر حتى لو من شبكة بعيدة وهو الأمر Ip helper address ونكتب على أي الـ gateway تكون للشبكة المراد الحصول على DHcp سيرفر منها ويكون الامر كالتالي

① تحديد الانترفيس المتصل به الـ Host

Router (config) # int F0/0 مثلا

② كتابة الأمر Helperaddress

Router(config-if) # ip helper address + dHcp server الـ IP الخاص بـ

أوامر الـ show الخاصة بـ DHcp هي

show ip dhcp pool - show ip dhcp binding - show ip dhcp conflict

clear ip dhcp conflict

ويمكن معرفة الـ IP الذي حصل عليه الجهاز عن طريق أمر على الـ Run

ipconfig /all

NAT

هي اختصار Network address Translation وقبل التكلم عنها لابد أن نعرف ماهو
private addressing وال Real Ips

① private addressing :-
هي مجموعة من العناوين التي تم حجزها للاستخدامات الخاصة داخل الشبكات المحلية
للمؤسسات أوفي الشبكات البيتية وسميت خاصة لأنه من المستحيل أن تجد جهازاً
أو سيرفراً متصلاً مباشرة على شبكة الانترنت يحمل واحداً من هذه العناوين
فهي غير مربوطة بأي نظام domain على الانترنت

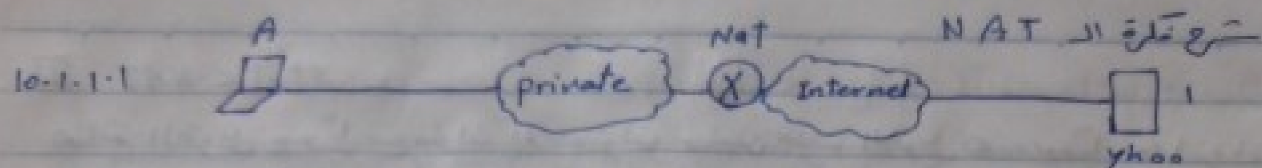
② هذه الايبهات الـ private تظهر الجدول التالي.

Range of Ip addresses	Class	Number of network
10.0.0.0 To 10.255.255.255	A	1
172.16.0.0 To 172.31.255.255	B	16
192.168.0.0 To 192.168.255.255	C	256

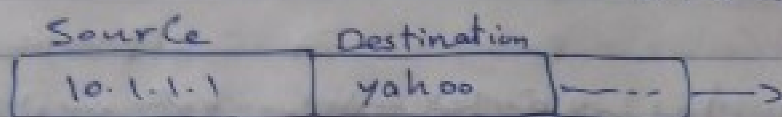
③ الـ Real Ips : هي الايبهات التي يمكنها الاتصال مباشرة بالانترنت.
دون الحاجة لوسيط.

فكرة عمل الـ NAT : هي تمكين أصحاب الـ private ips من الدخول على
الانترنت عن طريق تحويل private ip إلى real Ip
عند محاولة الدخول على الانترنت حيث أن الحصول على RealIp لكل جهاز
مكلف جداً . وبالتالي نحول الـ private سواء Ip واحد أو أكثر
إلى real Ip واحد أو أكثر من واحد.

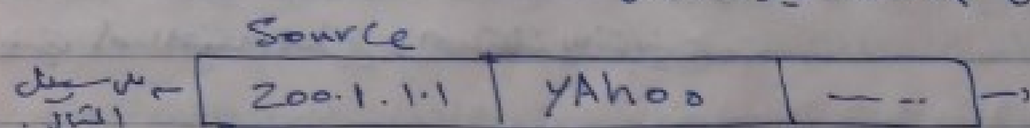
شرح فكرة الـ NAT



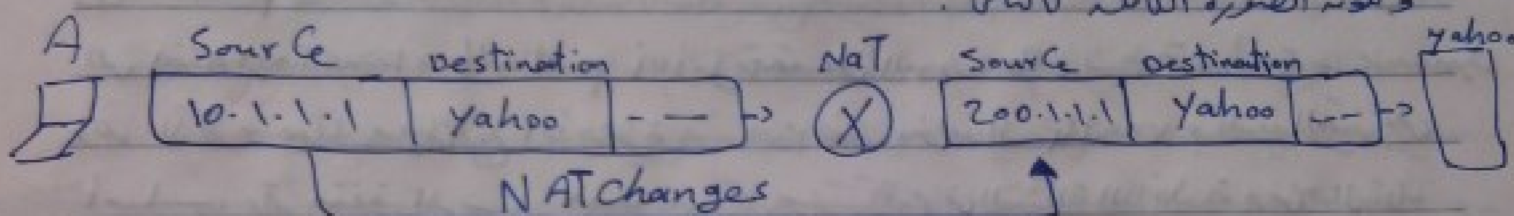
بفرض أن الجهاز A يريد الوصول إلى موقع yahoo فإن صورة الباكت الخارجة من A عندما تصل للراوتر تكون كالتالي



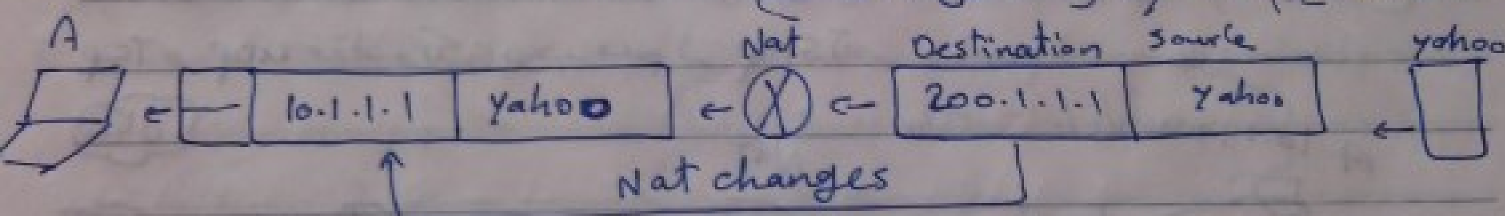
وعندما تصل للراوتر المفعل عليه الـ Nat يغير عنوان الـ Source وتحويله من private الواصل إلى Destination إلى real Ip فيكون كالتالي



وتكون الصورة الكاملة كالتالي.



وعندما يقوم yahoo بالرد نعكس العملية



* هذه الطريقة هي التي يتم صدقني سواء كنا نستخدم Ip واحد أو مجموعة من الأجهزة.

أنواع الـ Nat

Static
- Nat → one private ip ⇒ one real Ip
- pat : overloading : many Ip ⇒ one real Ip

Dynamic
- Nat → many Ip ⇒ many Ip
- pat → many Ip ⇒ many Ip : overloading

PAT = port address Translation

III Static NAT -:

هنا يتم التحويل يدوياً من عنوان إلى عنوان ونسمى عملية التحويل هذه يدوياً ومع ازدياد عدد الأجهزة تصبح العملية معقدة فكل جهاز يحتاج إلى IP real خاص به وهذا مكلف

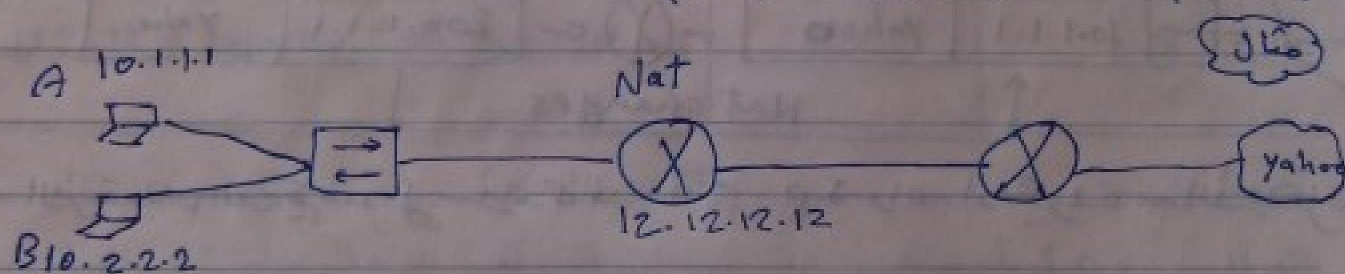
Dynamic Nat (2)

هنا يتم التحويل بين مجموعة من العناوين الخاصة بمجموعة أخرى من العناوين الـ real ويتم اختيار الـ IP real الذي سيخرج عليه الـ private بشكل عشوائي أي أي IP من مجموعة الايبيهات الـ real ولو كان عندي 20 جهاز يخرجون على 5 real لابد أن ينتظر الباقي حتى ينتهي أحد الخمسة ليخرج واحد مكانه للانترنت.

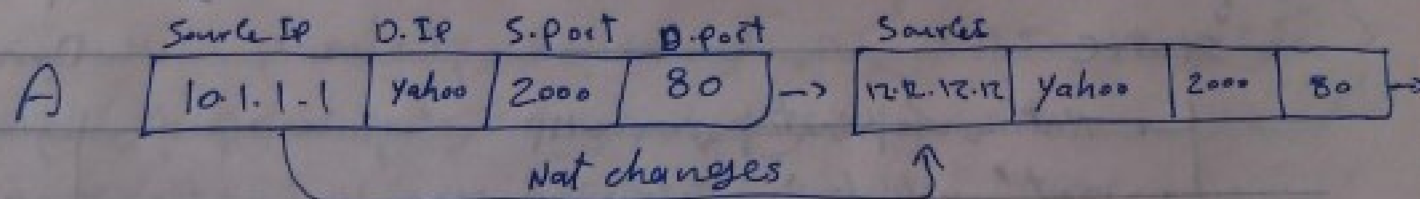
(3) pat -

هي اختصار port address translation أي أنه تعتمد على البورت وهي نسخة مطورة من Dynamic وهي الأكثر شيوعاً ففيها جميع الأجهزة تستخدم نفس عنوان الـ IP real وكذلك يتم التمييز على أساس رقم منفذ المرسل للتمييز بين كل مستخدم في الشبكة الداخلية وفي حال كان جهازين يستخدمون نفس المنفذ فإن الراوتر يغير أحد المنافذ وتعمل هذه الخدمة مع بروتوكول TCP و UDP فقط ولكن يوجد دعم لـ ICMP

(مثال)



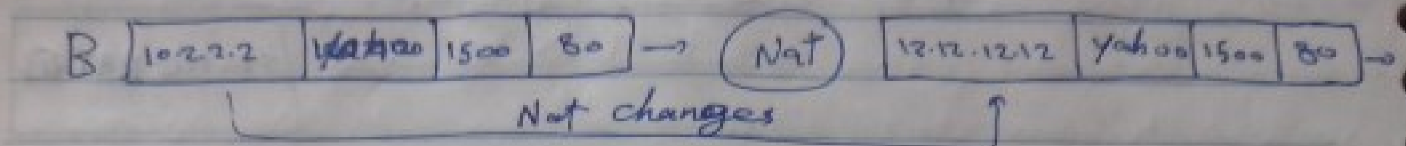
بفرض أن الجهاز A يرسل إلى yahoo فإن شكل الباكت يكون به المنفذ الذي خرج منه أي الذي يستخدمه الجهاز المرسل A ويحتوي أيضاً على البورت الخاص بالتصفح



نلاحظ أن الباكت احتوت على رقم منفذ كل من المرسل ويكون رقم بعد 1024 ورقم منفذ العملية أما المستقبل وهو 80 الخاص بالتصفح.

أي أن الـ pat تعتمد على البورت وبالتالي الجهاز B يستطيع استخدام

نفس الـ real IP لكن مع تغيير المنفذ كالتالي



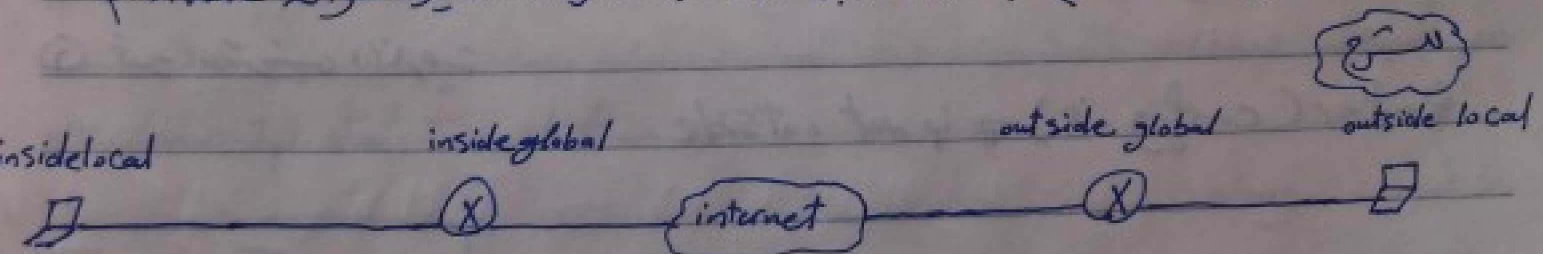
نلاحظ أنه الجهاز B (10.2.2.2) استخدم نفس الـ real IP وهو [12.12.12.12] ولكن استخدم بورت آخر غير بورت الجهاز A وهو 1500 في حين أنه الجهاز A استخدم 2000

- * في حالة أن الجهازين استخدما نفس المنفذ واختلفا المنفذ 2000 مثلاً فإنه الراوتر يخبر أحدهم أنه هذا المنفذ محجوز وبالتالي عليك استخدام غيره
- * علماً اختيار الجهاز للمنفذ الذي يخصصه يتم بشكل عشوائي لذلك قد تحدث الاستثناءات في المنفذ الذي يتغلب عليه الراوتر كان الخطوة السابقة
- * شرحنا هنا طريقة static pat أي استخدام real IP واحد لكل الأجهزة ولكن علماً الـ Dynamic pat أفضل حيث لا يحدث ضغط كبير على الـ real IP
- * علماً الـ pat تسمى أيضاً overloading حيث يتم تحميل عدد كبير من الـ private IP على الـ real IP.

مصطلحات هامة

1. Inside local ← الجهاز الداخلي في شبكتي الذي يكون عنوانه خاص private
2. Inside global ← الجهاز الداخلي "الراوتر الذي امتلكه" الذي يكون عنوانه real
3. outside global ← الجهاز الخارجي "الراوتر الثاني" الذي يكون عنوانه real
4. outside global ← الجهاز الخارجي في الشبكة الأخرى الذي يكون عنوانه private

للشرح



NAT Configuration

static NAT 1

① إنشاء الـ static NAT

Router(config) # ip nat inside source static + Private ip + real IP

② تعريف الانترفيس الداخلية

Router (config-if) # ip Nat inside

③ تعريف الانترفيس الخارجية "المتصل بالانترنت"

Router (config-if) # ip Nat out side

Dynamic NAT 2

① تحديد الـ Nat pool وتسميته وتحديد الـ range الخاص به ونكتب أول IP وآخر IP من الـ range

Router(config) # ip Nat pool + اسم + Frist IP from the range + end IP of range + netmask

Router(config) # ip Nat inside source list 50 اسم أو رقم + pool + اسم الـ pool

② انشاء Accesslist لتحديد من يستطيع استخدام الـ real IP

Router(config) # Access-list 50 permit + عنوان الشبكة + wild mask

③ تحديد الانترفيس الداخلية

Router (config-if) # ip nat inside

④ تحديد الانترفيس الخارجية

Router (config-if) # ip Nat outside

paT 3

PAT

② Static PAT

Router(config) # ip nat inside source static Tcp آي بي المرسل + رقم البورت [illegible] ١٠٢٤ + آي بي المستقبل + البورت الخاص بالعميل [illegible] [illegible]

③ Dynamic PAT

① إنشاء الـ pool وتحديد الـ range وتسمية الـ pool

Router(Config) # ip Nat pool + اسم الـ pool + أول IP في الـ range + آخر IP في الـ range + netmask

② إنشاء الـ Access-list

Router(config) # ip Access-list standard Ahmed مثلاً

Router(config-std-nAcl) # permit + الشبكة الداخلية المسموح لها + wildmask

③ تفعيل الـ [illegible] على الـ pool والـ Access list ووضع كلمة overload

Router(config) # ip nat inside source list Ahmed pool + اسم الـ pool + overload

④ تحديد الانترفيس الداخلية

(config-if) # ip nat inside.

⑤ تحديد الانترفيس الخارجية

(config-if) # ip Nat outside.

أوامر الـ Show

show ip Nat Translation

show ip Nat static

* أمر الـ clear

clear Ip Nat Translation.

* أمر Debug

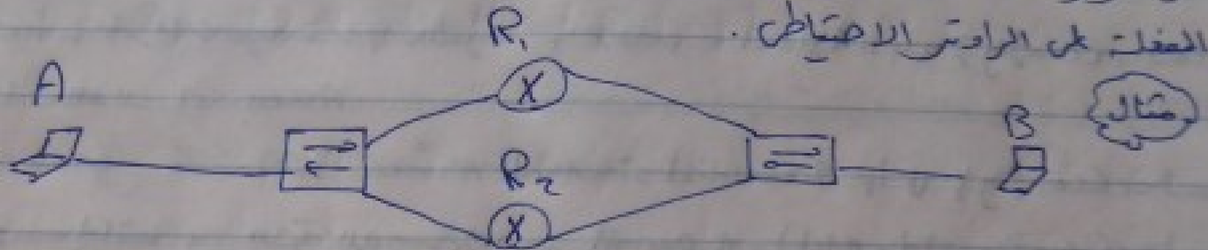
debug ip Nat

Frist Hop Redundancy Protocol

FHRP

يقوم هذا البروتوكول على توفير مسار بديل في حالة حدوث أي مشكلة في المسار الرئيسي وذلك عن طريق راوتر احتياطي للراوتر الرئيسي ويتم ذلك عن طريق إنشاء gateway وهمي على الراوتر الرئيسي وكذلك الراوتر الاحتياطي بحيث لو حدث أي مشكلة في الراوتر الرئيسي والذي عليه الـ gateway للشبكة تستخدم الشبكة الـ gateway المفعل على الراوتر الاحتياطي.

مثال



بفرض الجهاز A يريد أن يتصل بالجهاز B والـ gateway له هو البورت على الراوتر R_1 فلو حدثت مشكلة في هذا الراوتر يفقد الجهاز A القدرة على الاتصال B حيث أن الـ gateway الوحيد هو R_1 ففكرة FHRP هي كيفية الاستفادة من الراوتر R_2 عن طريق إنشاء gateway وهمي على كل من الراوترين تكون هي الـ gateway للجهاز A بحيث لو حدث مشكلة في الراوتر R_1 الراوتر الرئيسي يكون هناك مسار أو راوتر احتياطي تستطيع الشبكة استخدام الـ gateway الخاص به وهو بالطبع سيكون الـ gateway الوهمي المفعل على الراوترين في المثال حيث لا نستطيع أن نشير إلى أكثر من gateway حقيقية للشبكة وبالتالي لجأنا لإنشاء gateway وهمي مشتركة بين الراوترين.

أهمية FHRP

١- يحسن من قدرة الشبكة على العمل

٢- لو حدثت مشكلة يتغلب عليها عن طريق المسار الاحتياطي

* لإنشاء FHRP لدينا ٣ أنواع من البروتوكولات

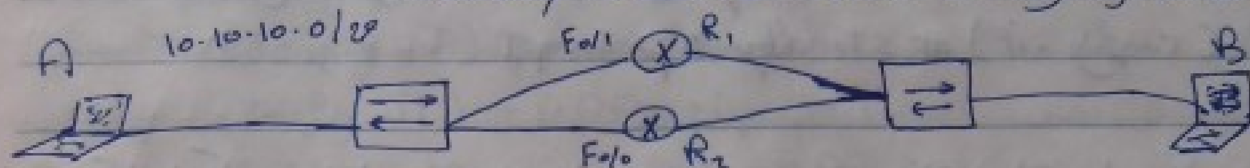
① HSRP

② VRRP

③ GLBP

HSRP ①

HSRP هي اختصار Hot standby Router protocol وهو بروتوكول خاص بسيسكو
حيث يكون راوتر يكون Active وهو الذي تنتقل من خلاله الداتا والراوتر الآخر يكون
في وضع standby أي في حالة استعداد للعمل في حالة حدوث أي مشكلة في الراوتر Active
يقوم هو بنقل الداتا من خلاله . هذه العملية تقوم بطرح أيضا getway وهمي
مشتركة في كلا الراوترين الـ Active وكذلك الـ standby



(مثال) بفرض في المثال السابق الجهاز A يرسل داتا للجهاز B ونريد أن نفعل
HSRP على الراوترين ماهي الاعدادات التي نقوم بها ؟

① اعدادات الراوتر R_1

Ⓐ ندخل على الانترفيس المواجه للسفيس ونعطيه IP من الشبكة

```
R1 (config) # int Fo/1
R1 (config-if) # Ip address 10.10.10.1 255.255.255.0
R1 (config-if) # No shutdown
```

Ⓑ نفعل أمر standby لتفعيل بروتوكول HSRP ونعطي العملية رقم ونضع الـ getway الوهمي المشترك

```
R1 (config-if) # standby 1 Ip 10.10.10.5
```

نلاحظ اخترنا رقم العملية هو (1) ويمكن اختيار غيره واخترنا الـ getway 10.10.10.5

Ⓒ تعديل الـ priority لجعل هذا الراوتر هو الرئيسي Active :

```
Router (config-if) # standby 1 priority 150
```

نلاحظ نكتب اسم العملية (1) حتى تفعل عليها هذا الأمر وبالنسبة للـ priority فإنه
في الأساس أو في الوضع الافتراضي 100 وبالتالي لكي نجعل الراوتر هو الـ Active نزيدها
عن الـ 100 وجعلناها 150

⑤ تفعيل الأمر preempt

فائدة هذا الأمر في حالة لو الـActive حصلت فيه مشكلة فإنه بعد انتهاء المشكلة وعودته للعمل فإنه الراوتر الآخر الذي كان standby سيكون هو الـActive في حالة سقوط الـActive الأساسي وبالتالي عند عودته للعمل فإنه لن يأخذ مكانه الأصلي بل سيكون standby والاحتياطي الذي أصبح أساسي سيكون ما زال أساسيًا فعند تفعيل هذا الأمر يجعل الراوتر الـActive لو سقط ثم عاد للعمل يرجع لحالته الأصلية Active ويرجع الآخر لحالته الأصلية Standby

R1(config-if) # standby 1 preempt

وهكذا نكون فعلنا HSRP على الراوتر R1 ونذهب لتفعيله على R2

R2 Config

R2(config) # int F0/0
R2(config-if) # Ip address 10.10.10.2 255.255.255.0
R2(config-if) # No shutdown
R2(config-if) # standby 1 Ip 10.10.10.5 الـvirtual gateway المشترك
R2(config-if) # standby 1 preempt

وهكذا نكون فعلنا HSRP وأما بالنسبة للأوامر الـshow

R1 # Show standby brief
R1 # Show standby

② VRRP

Virtual Router redundancy protocol.

هذا البروتوكول هو نفس فكرة بروتوكول HSRP لكن VRRP يعمل على كل الأجهزة بخلاف HSRP فهو يعمل على أجهزة سيسكو فقط وبالنسبة للأوامر فهي نفس أوامر السابقة لكن نستبدل Active لتكون Master وكذلك نستبدل standby لتكون Backup أي تكون الراوتر الرئيسي هو الـmaster والاحتياطي هو الـBackup

الاختلاف الثالث بين VRRP وبين HSRP يكون في الـ Configuration حيث يتم استبدال كلمة standby بكلمة VRRP

VRRP Config

```
Router(config)#int Fo1/1
Router(config-if)#ip address 10.10.10.1 255.255.255.0
Router(config-if)#no shutdown
Router(config-if)#VRRP 2 ip 10.10.10.5
Router(config-if)#vrrp 2 priority 110
Router(config-if)#VRRP 2 preempt
```

الوهمي getway

ونعمل نفس الاوامر على الراوتر الثاني وبالنسبة لأمر الشو show هو

```
Router#show VRRP.
```

GLBP ③

GLBP ⇐ هي اختصار getway load Balancing protocol وهو بروتوكول خاص بشركة سيسكو وهو يعمل على الطبقة الثانية Data link layer و HSRP و VRRP تعمل على الطبقة الثالثة Network layer

فكرة عمله: بالاضافة لفكرة إنشاء getway وهمي مشتركة بين الروترات فإنه ينشئ macaddress وهمي لكل راوتر ويكون الراوتر الرئيسي صاحب أعلى Priority فإن تساوت يكون صاحب أعلى IP ويكون الماك الخاص بكل بورت متصل بالشبكة على الشكل التالي 0007.B400.xxyy حيث يكون XX هو رقم المجموعة التي انشأناها و yy هي أرقام المناقذ على الشبكة فلو كان لدينا ثلاث روترات ورقم المجموعة هو 1 يكون الـ mac للراوتر الاول هو 0007.B400.0101 ويكون الراوتر الثاني 0102 والثالث 0103 وهكذا وكما قلنا يتم استخاب

راوتر رئيسي وهو صاحب الـ Briority ومعها صاحب أعلى Ip لو تساوت الـ Briority ويسمى الراوتر الرئيسي AVG ⇐ Active Virtual Getway ويقوم هو بتوزيع الماك الوهمي على الروترات فمثلا مرة يستلم ARp لمعرفة الماك أدريس يرسل ماك وهمي من الذي تم إنشائه فلو استلم أول Arp يرسل الماك الوهمي الخاص به وبالتالي يتم ارسال الداتا من خلاله والـ Arp الثانية يرسل الماك الوهمي للراوتر الثاني فيتم ارسال الداتا من خلاله وهكذا وبالتالي تحدث عملية الـ load Balance وهو أن يتم توزيع الاحمال على الروترات وبالنسبة للروترات الاخرى تسمى AVF ⇐ Active virtual Forward

GlBp Config

```
Router(config)# int Fo/0
Router(config-if)# Ip address 10.10.10.1 255.255.255.0
Router(config-if)# No shutdown
Router(config-if)# glbp 3 ip 10.10.10.5
Router(config-if)# glbp 3 priority 110
Router(config-if)# glbp 3 preempt
```

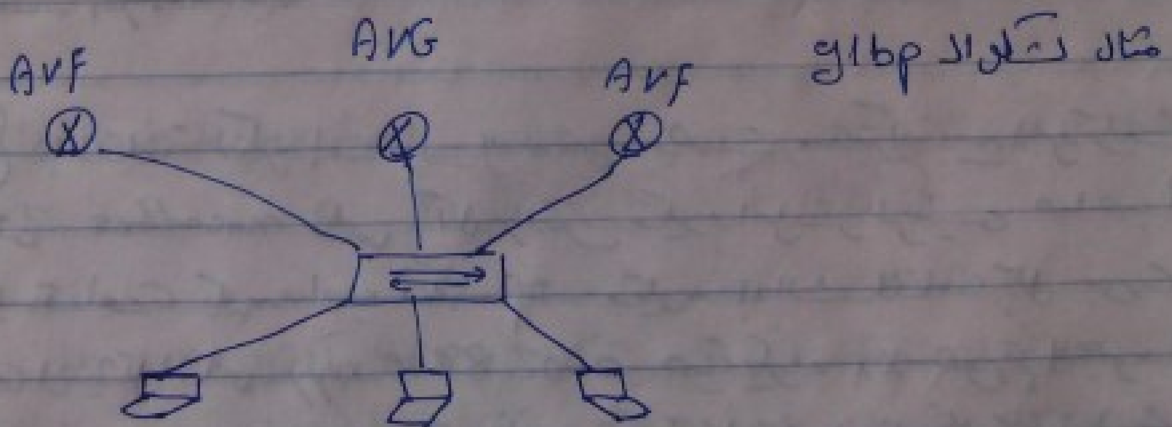
الـ [illegible] هو الـ الوهمية المشتركة

ونفعل ذلك على كل راوتر

أوامر الـ show

```
Router# show glbp
Router# show glbp brief or group - interface
```

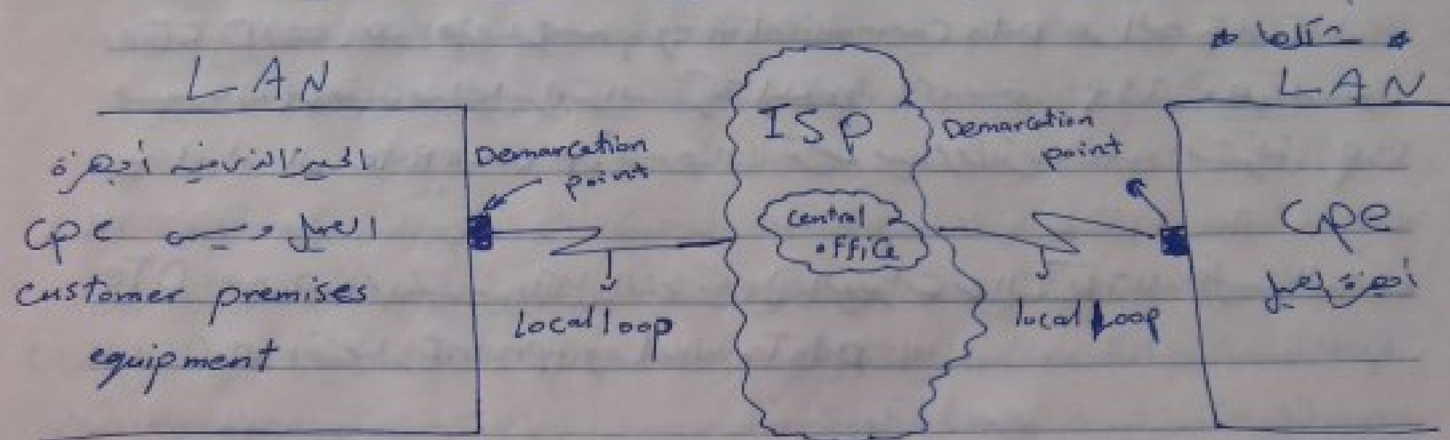
مثال لشكل الـ glbp



Wide Area Networking
WAN

شبكات الـ wan هي الشبكات التي تستخدم البنية التحتية للدولة أو شركات Isp في الربط بين أجزاء الشبكة المتناثرة وترتبط بين مناطق بعيدة.

* شكلها *



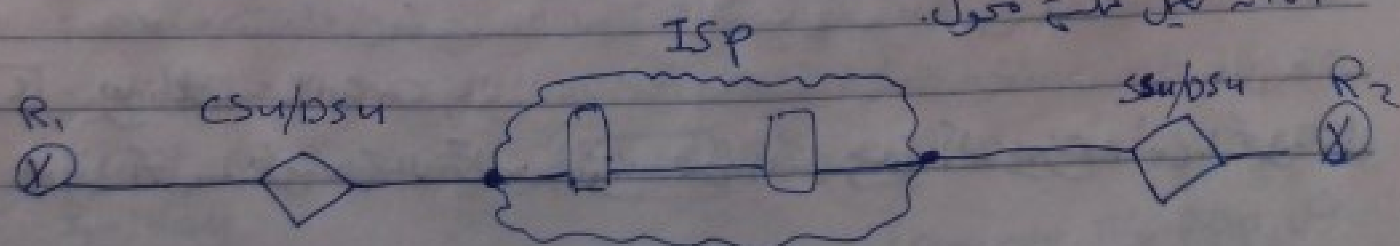
① (CPE) Customer premises equipment
المقصود بها الأجهزة التي تتواجد عند العميل وليس شركة الاتصالات أو Isp مثل DSLmodem وغيره من الأجهزة

② Demarcation point. ⟸ وهي الأجهزة أو النقطة التي تنتهي عندها أجهزة العميل (Cpe) وتبدأ خطوط شركات Isp عندها مثال الجهاز اسفل المبنى المتصل به كابل الهاتف مثلاً pstn هو بوكس اسفل المنزل يسمى public switched telephone network

③ Local Loop ⟸ المقصود بها الوصلة بين السنترال والسويتش الذي يوزع الخطوط للمبنى و~~pstn~~

④ (Co) Central office ⟸ المقصود به شركة Isp أو السنترال الخاص بك

⑤ CSU.DSU ⟸ channel serviceunit . Digital servicCeunit
جهاز يتم توصيل السيريال به ليتم الخروج منه على شكل كابل هاتف والعكس أي أنه يعمل عمل محول.



عن طريق جهاز CSU/DSU حتى نستطيع التحكم في السرعة المراد نقلها في الشبكة.
وجهاز ⟸ CSU/DSU. قد يكون مدمج في الراوتر عن طريق شراء كارت
خاص مثل HWIC-4T1/E1 , WIC

الـ DCE والـ DTE :

DCE ⟸ هو اختصار Data Communication equipment هو الجهة من كابل السيريال يحتاج توصيلها براوتر الشركة المزودة للخدمة ISP وهي المسؤول عن اعداد الـ Clock Rate حتى يكون هناك تزامن بين راوتر الخاص والشركة ISP

DTe ⟸ هو الجانب من الكابل الذي يتصل بالروترات في الشبكة الداخلية الـ Lan
وهو اختصار Data Terminal equipment

WAN Connection Types *

الأنواع التي أستطيع استخدامها داخل wan هي

① leased line — Circuit switched — packet switch

1 leased line "Dedicated"

هو عبارة عن خط مستأجر مخصوص بالشركة يعني أنني أحجز خط من الاتصال بين فرعين أو أكثر للشركة بحيث يكونوا متصلين ببعض على مدار 24 ساعة
الخط يكون خاص فقط بالشركة ولا يستخدمه أي شخص آخر وتكون سرعة الخط ثابتة على مدار اليوم وتلتزم شركات ISP بصيانته لكنه مكلف ماديًا ومن خصائص الـ leased line ⟸ أنه عبارة عن 1:1 أي سرعة التصفح والداونلود والابلود ثابتة لو تعاقدت مثلاً على 1 ميجا سيكون الكل واحد ميجا

2 Circuit switching

هو نوع آخر من طرق الاتصال تكون بطيئة من حيث السرعة لكن يميزها أنني أتحمل فقط

تكلفة ما تم استهلاكه ومن أمثلته Dial up وكذلك ISDN
وفكرة الـ Dial up عبارة عن رقم هاتف معين مثل 0777 5000 مثلاً هذا الرقم تحدده
شبكة من مشتركات [illegible] مثلاً للدخول على الانترنت ويقوم المستخدم الذي يريد الاتصال
بالانترنت بتركيب كارت فاكس في جهاز الكمبيوتر ويتصل بـ Rj 11 ويقوم بالاتصال
على هذا الرقم 0777 5000 والذي بدوره يكون متصل على الانترنت وبالتالي يستطيع المستخدم
الدخول على الانترنت لكن بسرعة بطيئة جداً أقصاها يكون 56 Kbps وبالطبع يستخدم
نظام [1:8] أي التصفح = السرعة كاملة عند الداونلود ثم 1/8 السرعة

ISDN ← هو يعتبر فكرة الـ Dial up ولكن أتحمل تكلفة ما استخدمته فقط
وهو باختصار جهاز يتم شراؤه وتقوم شركة الاتصالات بتزويدك بخدمة الانترنت يقوم
الجهاز بتقسيم الكابل الرئيسي إلى جزئين جزء خاص بالمكالمات الصوتية والآخر خاص بالداتا
والدخول على الانترنت يتم توصيله بالكمبيوتر وتكون سرعة الانترنت من الوصلة التي تصل
بجهاز الكمبيوتر هي 64 Kbps وعليه الاستفادة من أقصى سرعة 128 Kb في حالة
عدم الاستفادة من هاتف المكالمات.

* بالنسبة للبروتوكولات المستخدمة في Circuit switching هي
X.25 ، ppp ، Frame-relay ، ATM.
و ATM باختصار هو بروتوكول يستطيع نقل جميع أنواع الداتا مثل voice ، video
وغيرها.

3- packet switching
فكرته هو خليط بين مميزات التكلفة القليلة مثل Circuit switching والسرعة العالية
مثل leased line ويستخدم فيه جهاز DSLAM وهو اختصار للكلمة
Digital subscriber line access Multiplexer ولفهم كيفية عمله لابد أن
نعرف أن خطوط ADSL هي خدمة انترنت محملة على خطوط الهاتف ويقوم بعملية الدمج
هذه جهاز Dslam يتم وضعه في السنترال توصل إليه خطوط الهاتف من جهة
ثم تخرج من الجهة الأخرى خطوط ADSL يأخذ السلام واحد منها مثلاً ثم يقوم بتوزيعها
على المشتركين وتكون السرعة بنظام [1:8] ويستخدم نظام الـ packet switching بروتوكولات
مثل ppp والـ Frame relay

عيوب packet switching هو انك تتأثر باستخدام الخطوط يعني لو كنت استخدم الانترنت لوحدي افضل ما استخدمه انا وغيري على نفس الشبكة.

* بالنسبة لـ DSL فهو اختصار Digital Subscriber line وهي من اهم تقنيات الاتصال التي ظهرت حديثاً لاتاحة سرعات أكبر بالاتصال للانترنت وهو المستخدم حالياً بكثرة حيث كان يستخدم قبله تقنية ISDN التي كانت أكبر سرعة توفرها 128Kb

وينقسم الـ DSL إلى نوعين

ADSL	SDSL
Asymmetrical DSL	Symmetrical DSL
تكون فيه سرعة الداونلود أكبر من سرعة الـ upload ومعناه خط اشتراك رقمي لا تناظري	خط اشتراك رقمي تناظري أي ان سرعة الداونلود = سرعة الـ upload

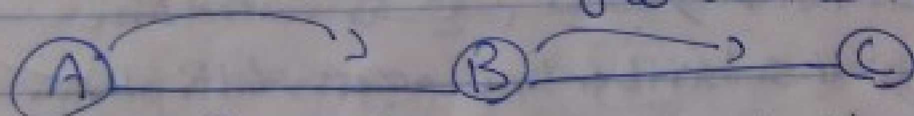
WAN protocols

① بروتوكول HDLC

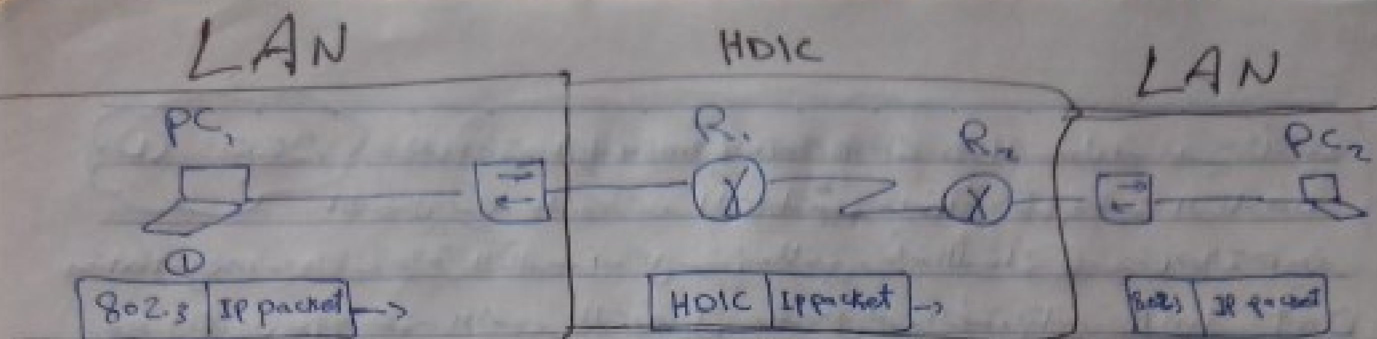
HDLC هو اختصار لـ High level Data-link Control وهو بروتوكول الـ Default على أجهزة سيسكو اي انه لم تحتاج لضبطه على أجهزة سيسكو حيث انه بالفعل يعمل بصورة مباشرة على أجهزتها وينقسم إلى نوعين Cisco HDLC وهو فقط الذي يعمل على أجهزة سيسكو ونوع آخر ISO HDLC ويعمل على الأجهزة الأخرى بخلاف سيسكو

فكرة عمله

ابتداء نلاحظ المثال التالي



في حالة ارسال A إلى C فإن الـ Frame يرسل إلى B ابتداءاً ويكون متضمن الـ macaddress في عملية الـ encapsulation فكرة HDLC هي انه في عملية الـ encapsulation فإنه لا يضع macaddress ولكنه يضع في عملية encapsulation تعريف HDLC أي سيتم استخدام بروتوكول HDLC ويتضح ذلك بالمثال



* فائدة كابل السيريال أنه مش صعب تقطع من الكابل فإنه يشغله حتى لو كان من الكابل بين السنترالات أو كابل ISP خصوصا أنه الكابل من الـ LAN بيتم تقطيعه الـ ethernet فلا يشعر بالنسبة السنترالات وبالتالي استخدم السيريال في الـ WAN حيث أنه أفضل في عملية الـ Troubleshooting ولذلك تم ضبطه على

عيوب HDLC : لا يمكن استخدامه بين الأجهزة المختلفة.
لا يتم عملية التوثيق الـ Authentication ويستخدم فقط في leased line

ميزة : ① أنني لا أحتاج إلى تفعيله على أجهزة سيسكو لأنه By default موجود عليها وبالنسبة إلى الأجهزة غير سيسكو نحتاج فقط ضبط الـ encapsulation وتحديد نوعها HDLC.

② بروتوكول HDLC هو البروتوكول الأسرع على الإطلاق حيث حجم الـ Header صغير في الـ packet

② بروتوكول PPP

PPP هو اختصار لـ point-to-point protocol نستنتج من اسمه أنه لوصل نقطتين ببعضهما مثل HDLC ويعتبر PPP أكثر البروتوكولات استخداما في العالم كونه أغلب مستخدمي الإنترنت يعتمدون عليه للوصول إلى الإنترنت من خلال الاتصال مع شركات ISP والتي تتم من خلال بروتوكول PPP وتعود شهرة PPP أيضا أنه يستطيع العمل مع أجهزة الراوترات المختلفة بعكس HDLC على العكس لا يسمح بأجهزة روترات مختلفة.

* ينقسم بروتوكول PPP إلى

Link control protocol [LCP]

Network Control protocol (NCP)

① LCP

هو اختصار Link Control protocol وهو المسئول عن عملية تأمين الاتصال بين النقطتين المتصلتين بمعنى آخر يقوم بعملية التفاوض negotiation مع الطرف الآخر للتأكد من أن كل شيء مطابق وبأن الليك بينهم في حالة جيدة وهذا الجدول يوضح هذه الأمور بالتفصيل وهو يعمل ضمن الطبقة الثانية Dat_link

Link Quality Monitoring (LQM)	فيه يتم تبادل الاحصائيات حول نسبة الحزم التي وصلت بدون اخطاء
Looped link detection	يقوم lcp بتوليد رقم عشوائي يسمى magic number مؤلف من أربع بايت بلغة الهيكسا ويقوم بإرساله في حال استلم هذا الرقم مرة أخرى يدرك أنه يوجد Loop وبالتالي يتم توقيف الليك
Layer 2 loadbalancing multilink	فيه يتم التفاوض مع الطرف الآخر من أجل توزيع الترافيك في حالة لو كان هناك أكثر من لينك يصل النقطتين وبالتالي الاستفادة من خاصية الـ loadBalancing
Authentication	وهي من اجل التأكد من التوثيق والتوافق بين النقطتين وهما نوعان pap و chap

② NCP

هو اختصار Network Control protocol وهو مسئول عن إدارة عملية الـ encapsulation بين النقطتين وبالتحديد اداره بروتوكولات الطبقة الثالثة Network

Authentication protocols

تنقسم بروتوكولات التوثيق إلى نوعين

CHAP | PAP

* الفرق بين

password Authentication protocol	challenge Hand Authentication protocol
PAP	CHAP
يرسل كلمة المرور واليوزر بصورة صريحة وغير مشفرة cleartext	يرسل كلمة المرور واليوزر مشفرة (Encrypted)
أقل قوة	أكثر قوة
رسائل ثنائية	رسائل ثلاثية

* شكل ال PAP

Tarek (X) ← ① I Am Ahmed / password = 1234 — (X) Ahmed

(X) ② ACK → (X)

شكل ال CHAP

Tarek (X) ① challenge → (X) Ahmed

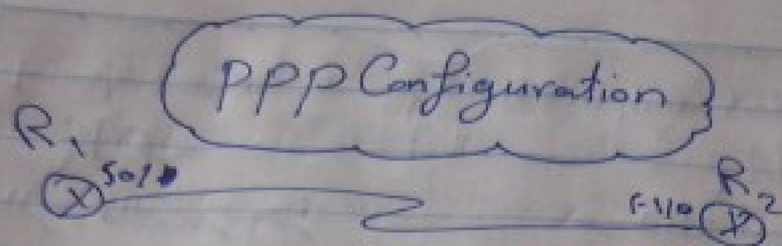
(X) ← I Am #$%$#@ ② (X)

(X) ③ Accepted → (X)

* بروتوكول PAP ⟸ يتألف هذا البروتوكول من عمليتين اساسيتين ① طلب التوثيق Authentication Request يرسل الجهاز المنشأ للاتصال طلب توثيق فيه اسم مستخدم وكلمة مرور ② رد التوثيق Authentication reply فيؤكد الجهاز الآخر ما إذا كان سيقبل الجهاز الأول اعتماداً على اسم المستخدم وكلمة المرور

* بروتوكول CHAP ⟸ لا يرسل كلمة المرور وانما يقوم الجهاز فيه بتطبيق عملية حسابية على كلمة المرور ومن ثم التأكد من نتيجة هذه العملية للتحقق من مطابقة كلمة المرور

PPP Configuration



CHAP ①

Router 1

```
Router(config)# hostname R1
Router(config)# int Serial 0/0
Router(config-if)# encapsulation ppp
R1(config-if)# username + اسم الراوتر الثاني + password 123 مثلا
R1(config-if)# ppp Authentication CHAP
```

R2

```
Router(config)# hostname R2
Router(config)# int serial 1/0
R2(config-if)# encap ppp
R2(config-if)# username + اسم الراوتر الأول + password + 123
R2(config-if)# ppp Authentication Chap
```

PAP ②

نفس فكرة ال chap لكن نضيف امر ارسال ال password

R1	R2
Router(config)# hostname R1	Router(config)# hostname R2
R1(config)# int serial 0/0	R2(config)# int serial 1/0
R1(config-if)# encap ppp	R2(config-if)# encap ppp
R1(config-if)# ppp Authentication pAp	R2(config-if)# ppp Authentication pAp
R1(config-if)# ppp pAp sent-username R1 password 123	R2(config-if)# ppp pAp sent-username R2 password 123

أوامر الـ show

Router # debug ppp negotiations

Router # debug ppp packets

Router # debug ppp erros

Router # debug ppp Authentication

Router # show interfaces serial 0/0/0

* بعض أنظمة التشغيل للروترات قد لا تحتوي على أحد الأنظمة pAp أو chap

وبالتالي نستخدم البعض أو جميع بحيث لكي يستخدم الراوتر البروتوكول في حالة عدم وجود الآخر

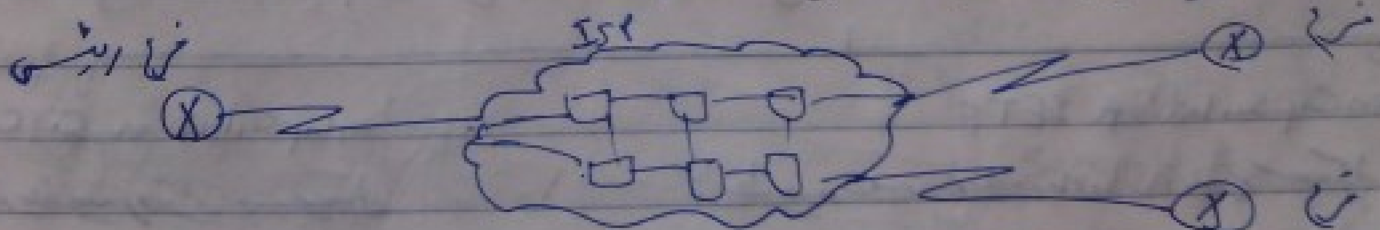
Router (config-if)# ppp authentication chap pAp

Frame Relay

تقنية الـ Frame relay هي خدمة تقدمها شركات ISP للشركات والمؤسسات المختلفة عن طريقها تستطيع تلك المؤسسات ربط أكثر من فرع إلى نقطة مركزية واحدة مثل البنوك . وتعتبر تقنية الـ Frame-relay من أشهر تقنيات الشبكات الممتدة الـ WAN وهي تتمتع بالآتي :-

1. رخص الثمن مقارنة بخطوط الـ leased Line
2. Shared Bandwidth

شكلها تتكون الشبكة الـ Frame-relay من فرع رئيسي وفروع فرعية يتم الربط بينهم عن طريق البنية التحتية لشركات ISP



* الأجهزة في ISP الخاصة بتقنية الـ Framerelay تسمى Frame-relay سويتش أو روترات يتم تعريف بعض الأوامر عليها التي تسمح أن يكون الفرع الرئيسي والفروع الأخرى ضمن شبكة واحدة .

(فكرة عملها) تقوم فكرة عمل الـ Frame relay على انشاء مسارات وهمية.
يتم استخدامها بدل استخدام leasedline ذو التكلفة المرتفعة.
هذه المسارات الوهمية يتم ربط الفرع الرئيسي بفرع واحد فقط على كل مسار

(مثال)



المسار من القاهرة للاسكندرية هو مسار وهمي ومن القاهرة لطنطا مسار وهمي آخر منذ الأصل وهي مسارات وهمية لأنه في الاصل هذه المسارات لم يتم تخصيصها لهذه الفروع والفرع الرئيسي ولكنها مسارات تستخدمها شركات الـ ISP لربط المناطق ببعض وتم استخدامها عن طريق بعد السادات الـ Config لترتبط فروع القاهرة باسكندرية والقاهرة بطنطا وفي نفس الوقت ترتبط فروع شركات أخرى خصوصية أن الـ leasedline لا يكمن أن يستخدمه أي شركة أخرى غير الشركة المتعاقدة عليها. هذه المسارات الوهمية تسمى PVC سنتكلم عنها لاحقا.

* نلاحظ من الشكل أن الـ Frame relay عبارة عن جزئين الـ cloud والمسئولة عن السادات هذا الجزء هي شركة ISP ويتم دراسة هذا الجزء في ccnasp
* أما الجزء الأخر فهو روترات المركز الرئيسي والفروع المختلفة وهو ما تتناوله شهادة CCNA و CCNP Routing and switching

Frame-relay encapsulation

الراوتر يكون مفعل عليه HDLC encapsulation في البداية ولكي نفعل عليه تقنية الـ Frame relay فإننا نحتاج إلى تفعيل Frame-relay encap عليه وتنقسم إلى

encapsulation Cisco
تربط بين روترات سيسكو

encapsulation IETF
تربط بين نوعين مختلفين بالاضافة لجهاز سيسكو

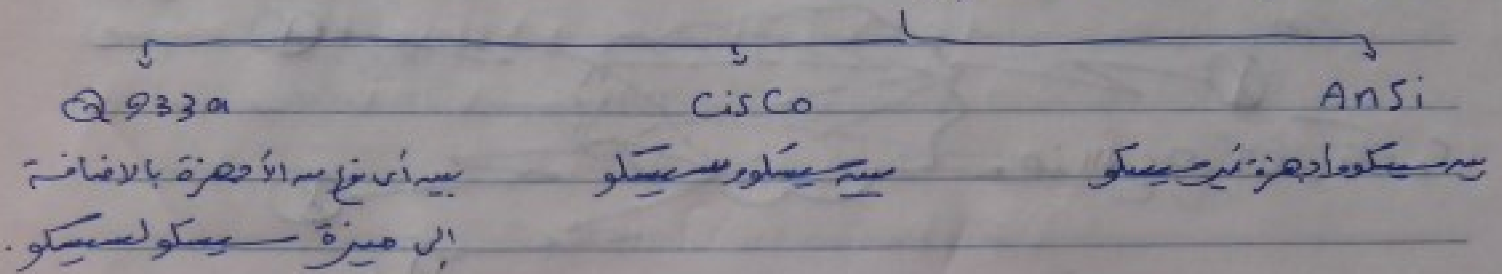
PVC

هو اختصار permanent virtual circuit وهي عبارة عن المسارات الوهمية

التي تربط المركز الرئيسي والفروع داخل الـ cloud وبمعنى آخر هي اللينكات بين الـ FR switch داخل الـ cloud

LMi

هي اختصار Local management interface وهي عبارة لغة التعامل بين الروترات والـ FR switch وهي تتحكم بتغيير الـ Bandwidth وكذلك هو المسئول عن جعل كل فرع يتصل بالمركز الرئيسي بصورة مستقلة مع انه من الأصل كابل واحد فعلي وكذلك يحدد نوع الـ encapsu وينقسم الـ LMi إلى



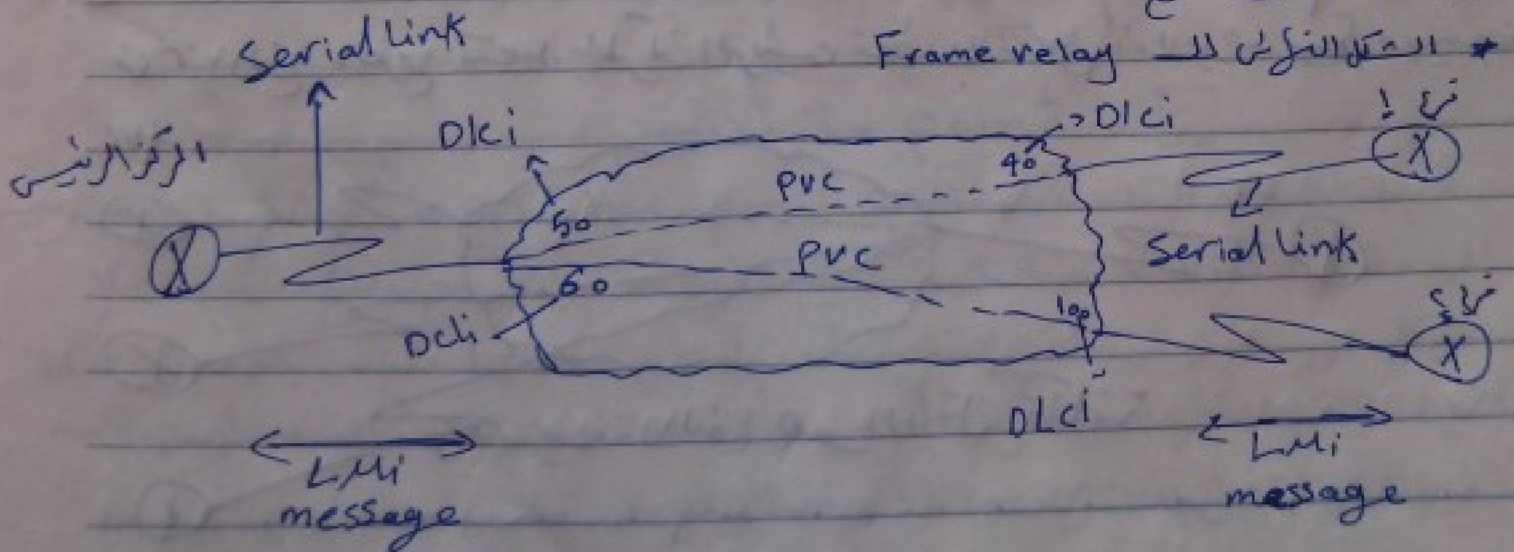
بين سيسكو وأجهزة غير سيسكو | بين سيسكو وسيسكو | بين أي نوع من الأجهزة بالإضافة إلى ميزة سيسكو لسيسكو.

CIR # هو الحد الأدنى لسرعة الخط Committed information rate
PIR # الحد الأعلى لسرعة الخط Primary information Rate

DLCi

هو رقم تعريف عن طريقه يتم تحديد المسار الذي ستمر به الداتا.
يتم وضع رقم الـ DLCi على رأس كل مسار وهي PVC ويكون حيز الأرقام بين ١ من ١٧ ويصل إلى ١٠٠٠ لا يتشابه رقم DLCi وآخر عند المركز الرئيسي وكذلك قد يتشابه رقم DLCi بين الفروع

* الشكل التالي للـ Frame relay

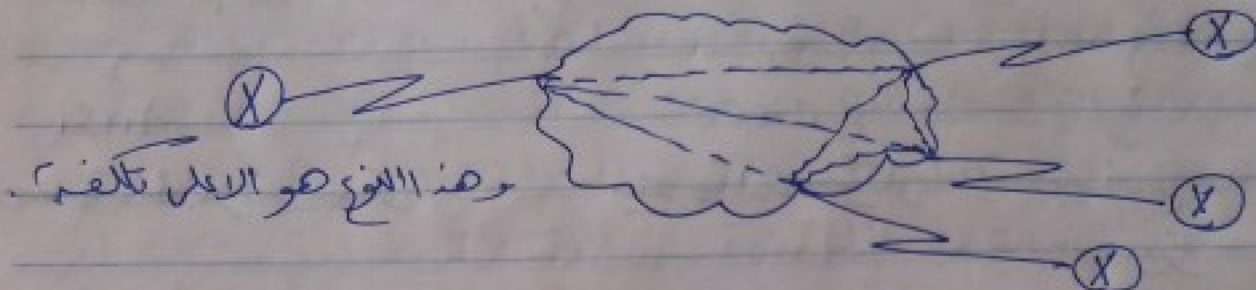


Frame relay Topology

① mesh Topology — ② partially Topology — ③ hab and spoke

① Mesh Topology

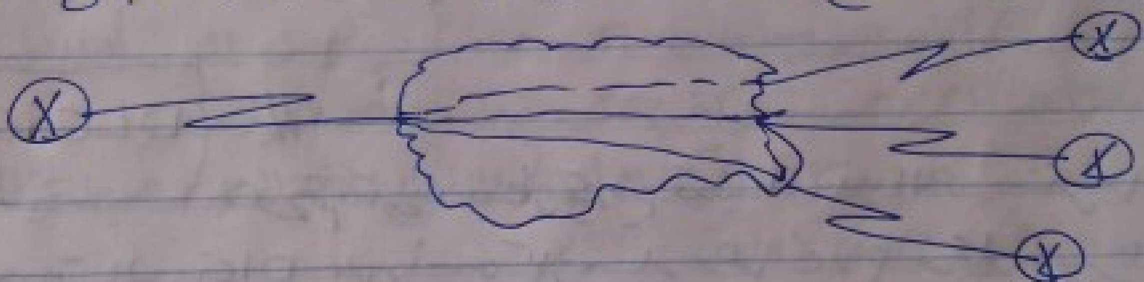
في هذه التوبولوجي المركز الرئيسي وكل الفروع متصلة ببعضها البعض أي بين كل فرع والآخر وبين كل فرع والمركز الرئيسي PVC كالتالي



وهذا النوع هو الأعلى تكلفة.

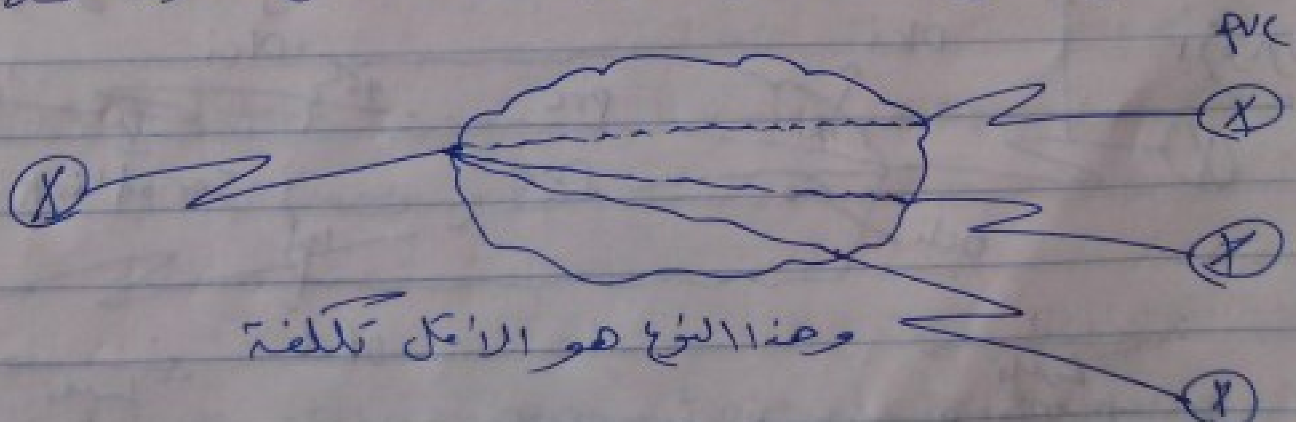
② partially Topology

في هذا النوع ليس كل الفروع متصلة ببعضها البعض بـ PVC وتكون بعضها متصل كذلك



③ hup and Spoke

في هذا النوع الفروع تتصل بالمركز الرئيسي فقط ولا تتصل أو لا يوجد بينها وبين بعض PVC



وهذا النوع هو الأقل تكلفة

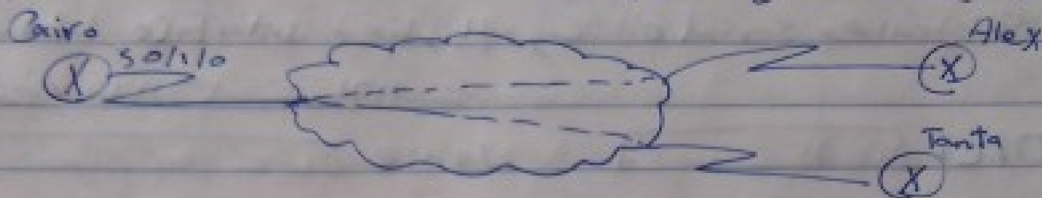
Frame-relay Configuration

تنقسم ال Frame relay من حيث التطبيق العملي و الاعدادات إلى نوعين

① point to multipoint ② point to point.

1 point to multipoint

في هذا النوع أفرع الشركة لا تستطيع التواصل مع بعضها في حين أنها تتواصل مع المركز الرئيسي بنجاح ولفهم ذلك



نلاحظ أن فرع الاسكندرية عند ما يريد التواصل مع فرع طنطا فإنه لابد أن يمر على المركز الرئيسي حيث أنه لا يوجد PVC بين الاسكندرية وطنطا مباشرة لذلك تذهب الداتا إلى الفرع الرئيسي ولكنها لا تخرج منه اتجاه طنطا وذلك بسبب خاصية ال split Horizon التي تمنع خروج الداتا أو ال update من نفس المخرج الذي استقبلت منه الداتا أو ال update وبالتالي لا تستطيع الفروع في هذا النوع multipoint التواصل مع بعضها إلا إذا كان هناك PVC يربط الفروع ببعضها ولكن كل PVC له تكلفة مما يجعل نوع multipoint عالي التكلفة.

* في هذا النوع "multipoint" تكون الفروع والمركز الرئيسي عبارة عن نفس الشبكة أي لها أيضا من نفس الشبكة ونفس ال Subnetmask

2 point to point

في هذا النوع يتم التغلب على خاصية ال split Horizon عن طريق تقسيم الانترفيس إلى subinterfaces وبالتالي تستطيع الفروع أن تتواصل مع بعضها بعضا كل وكل فرع يعتبر شبكة خاصة به أي أن كل فرع له Ip من شبكة غير الشبكة الخاصة بالفرع الآخر أو بالمركز الرئيسي وهذا النوع أقل تكلفة من multipoint وبالتالي تفضل الشركات استخدامه

Frame-Relay Implemenation

192.168.10.1 Cairo S0/0/0 — S0 20 / 50 — 20 S1 — S0/1/0 Alex 192.168.10.2 — 50 S2 — S0/1/1 Tanta 192.180.10.3

(P) إعدادات الـ Cloud على ← packet Tracer

① نذهب على برنامج الـ packet Tracer ونضغط على الـ cloud ونختار Config

② نذهب لخيار Interface ونختار البورت Serial 0 وهو المتصل بالقاهرة

③ ستظهر لنا الشاشة التالية

Dlci [ ] Name [ ]

[Add] [Remove]

④ نكتب رقم الـ Dlci وما يقابله من اسم الفرع مثال Dlci 20 والاسم الاسكندرية

Dlci [20] Name [Alex]

ثم نضغط Add

⑤ نكتب الـ Dlci الأخرى وما يقابلها ونضغط Add

* استكمالاً البورت Serial 0 نختار بعدها بورت آخر ونتبع نفس الخطوات نضيف الـ Dlci وما يقابله من الفرع

⑥ نضغط الآن على خيار Framerelay الموجود في قائمة الخيارات في عمود الـ Config الخاص بالـ cloud

* ستظهر هذه الشاشة

[Serial 0 ▼] [Alex ▼] [Serial 1 ▼] [Cairo ▼]

⑦ نختار سيريال 0 ونختار اسم أحد الفروع ثم نختار اسم السيريال الخاص بالفرع سيكون سيريال 1 ونختار الفرع الرئيسي القاهرة أي أننا عرفنا أن السيريال 0 له اتصال pvc طريق Alex ويقابله سيريال 1 الذي عن طريقه تتصل Alex بالقاهرة. ثم نضغط Add لتعريف المسار.

* نكرر العملية نختار serial0 لكن هذه المرة نختار الفرع الآخر طنطا

serial0 | TanTa | serial 2 | Cairo

عرفنا ال PVC الثاني سيخرج لفرع طنطا الذي يتصل بالقاهرة عن طريقه serial 2
ثم نضغط Add

(ب) اعدادات الروترات.

نذهب الآن لكل راوتر ونتبع الآتي.

① Cairo

```
Router(config)#host cairo
Cairo(Config)#int s0/0/0
Cairo(config-if)# No shutdown
Cairo(Config-if)#enCapsulation Frame-relay
Cairo(Config-if)# ip address 192.168.10.1 255.255.255.0
```

② Alex

```
Alex(config)# int s0/1/0
Alex(config-if)# no Shutdown
Alex(config-if)#ip address 192.168.10.2 , 255.255.255.0
Alex(config-if)# enCapSulation frame-relay
```

③ TanTa.

```
TanTa (config)# int s0/1/1
Tanta (config-if)#No shutdown
Tanta (config-if)#ip address 192.168.10.3 255.255.255.0
Tanta (config-if)#enCapSulation frame-relay
```

بهذه الطريقة نكون فعلنا الـ Framerelay على الروترات ونستطيع استخدام أوامر الـ show للمراقبة

Router#Show Frame-relay pvc
Router#show frame-relay map
Router# show Frame-relay LMi

• فكرة الـ map

فكرة أنني أستطيع أن أعلم الانترفيس لكي يرى الانترفيس المقابل عن طريق رقم الـ DlCi الخاص به كنوع من زيادة التأكيد

مثال نزيد في المثال السابق تأكيد أنه يرى الانترفيس 0/0/0 الخاص بالقاهرة في الاسكندرية عن طريق الأي بي 192.168.10.2 عن طريق رقم DlCi الخاص به وهو 20 وإذا أخذنا مثلا راوتر القاهرة. سيكون الأمر كالتالي

Cairo(config-if) # Frame-relay map Ip الخاص بالانترفيس المقابل + رقم DlCi الخاص به

Cairo(config-if) # Frame-relay map Ip 192.168.10.2 20

أمر الـ map هو أمر يدوي لربط رقم DlCi بعنوان أي بي وأما الأمر الديناميكي فيكون عن طريق بروتوكول IARP inverse address resolution protocole

IARP أو ما يسمى الـ inverse ARp هو اختصار بروتوكول يقوم بربط رقم الـ DlCi بعنوان IP المقابل أو بمعنى آخر يعرف كل DlCi ما يقابله من عناوين IP ويظهر في أمر show FR map بأنه Dynamic أما عند كتابة أمر MAP يدويًا يظهر أمامها static

أمر # show FR LMi يعرض نوع الـ LMi المستخدمة سواء كانت
- cisco
- Ansi
- Q.933A.

أمر show FR pvc يعرض الـ pvc التي قمت بها وكل DlCi ورقمه ويعرض حالة اتصال الـ PVC سواء

PVC status

Active

معناه يعمل بصورة سليمة ومتعرف على طرفي الـ PVC والـ DLCI الخاص بكل طرف

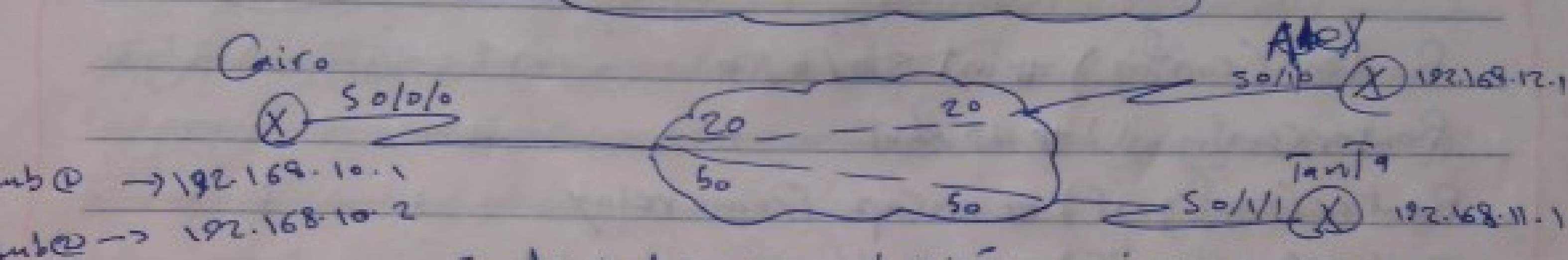
Inactive

معناه انه متعرف على طرف من PVC والآخر لم يتعرف عليه حتى لكنه لا يوجد خطأ فقط قد تكون في مرحلة التعرف عليه

Deleted

معناه انه يوجد مشكلة في DLCI او PVC

point to point Config



فانتم تقسيم الانترفيس الرئيسي للراوتر إلى Subinterface

① Cairo

(ممكن اي رقم)

```
Cairo(config)# int S0/0/0.15 point-to-point
Cairo(config-if)# No shutdown
Cairo(config-if)# ip address 192.168.10.1 255.255.255.0
Cairo(config-if)# encapsulation Frame-relay
Cairo(config-if)# Frame-relay interface-dlci 20
```

ونغير الـ IP في Subinterface الثانية ونكتب أمر DLCI الخاص بها

بالنسبة للفروع لا تحتاج إلى تقسيمها إلى Subinterface ولكن لا مانع أيضاً من تقسيمها.

ونستخدم أمر map للتأكيد أو كان نظام التشغيل لا يدعم inverse ARP

```
Cairo(config-if)# Frame-relay map IP 192.188.12.1 20 Broadcast
```

LMi Type

نستطيع من خلال بعض الاوامر تفعيل نوع معين من انواع LMI الثلاث سواء

- Q.933a
- Cisco
- ansi

ما الأمر هو

Router (config-if) # Framerelay LMi-type اسم النوع

مع مراعاة أنه يتم تفعيله من جميع الروترات في الـ Topology وأيضا إذا لم تعرف نوع LMi فإنه Bydefault يستخدم الـ CISCO

خلاصة الاوامر

Mutipoint

Router(config) #int S0/0/0
Router(config-if) #No shut
Router(config-if) # encap framerelay
Router(config-if) #ip address ______________
Rater (config-if) #frame-relay lmi-type ______ اسم النوع
Router(config-if)#Frame-relay interface-dlci ______ رقم الـ dlci

point-to-point

تقسيم الـ interface إلى Subinterface

Router(config) #int S0/0/0.رقم__ point-to-point

أمر الـ map

Router(config-if) #Frame-relay map ip Nexthop + Dlcinumber Broadcast

#Show FR pvc
#Show interface
#Show FR map
#Show Frame LMi

Virtual private Network (VPN)

ال VPN : هي تقنية لربط الشبكات البعيدة ببعضها عن طريق الانترنت بحيث يتم إنشاء قناة آمنة يتم فيها تمرير البيانات بطريقة مشفرة وتلجأ الشركات لتقنية ال VPN لانها أوفر في التكلفة من خدمات ال leased line وال Frame-relay في حين ان تلك الخدمات تقدم مستوى آداء وسرعة أعلى من ال VPN

* الشبكة الخاصة الافتراضية (VPN) تقدم حل للمشاكل الأمنية التي تواجه مستخدم الانترنت. حيث تقدم الآتي

① Confidentiality "privacy"

السرية أو الخصوصية حيث تقوم على منع أي شخص غير مرخص أو مرغوب فيه من قراءة البيانات والاطلاع عليها وهي المسئولة عن عملية التشفير

② Authentication

المصادقة :- هي عملية التوثيق التي تضمن لنا أن الطرف الآخر من VPN هو الطرف المقصود فعلاً وليس هاكر يتظاهر بأنه الطرف

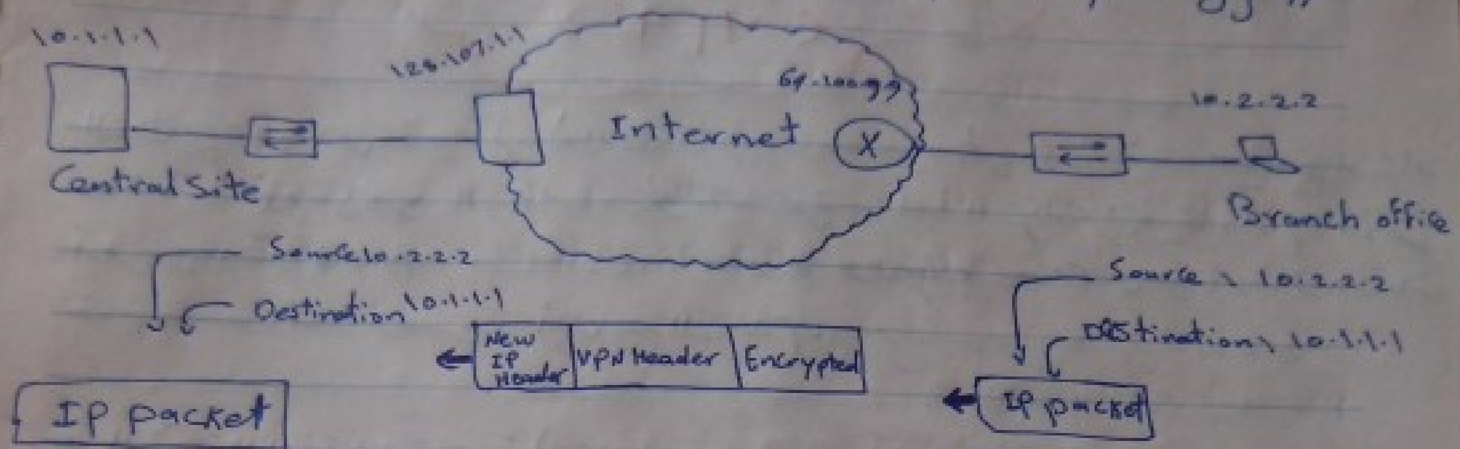
③ Data Integrity

سلامة البيانات :- هذه العملية تضمن لنا أنه لم يتدخل طرف خارجي وقام بتغيير أو تعديل في البيانات المرسلة وهي المسئولة عن عملية الهاشينج #

④ Anti-replay

منع إعادة الارسال :- وهو منع الهاكر من نسخ الداتا وإعادة ارسالها مرة أخرى حيث لا يقبلها المستقبل لأنه استقبلها مرة سابقة وبالتالي لا يستقبلها من الهاكر الذي يقوم بإرسالها حتى يحاول خداع المستقبل أنه شخص موثوق فيه.

VPN Topology



Types of VPN

Remote Access

يسمح لأفراد الشركة بالدخول من بعد لنظام الشركة سواء من البيت أو أي مكان آخر.

Site to Site

يربط بين موقعين للشركة مثل المركز الرئيسي مع فروع الشركة الأخرى

Intranet

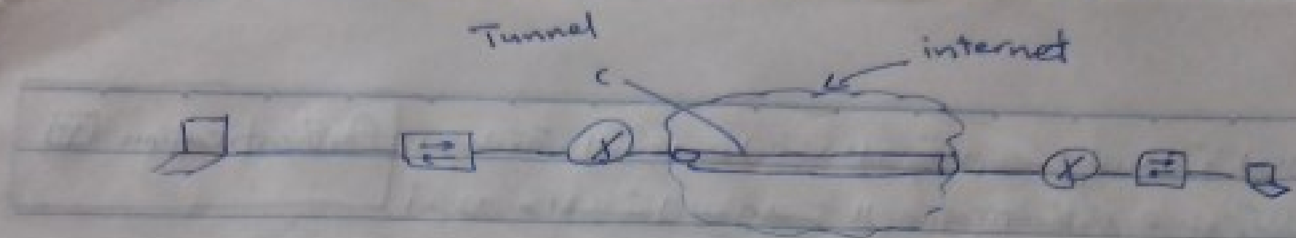
هو ربط جميع أجهزة الكمبيوتر الخاصة بموقعين مختلفين لنفس الشركة

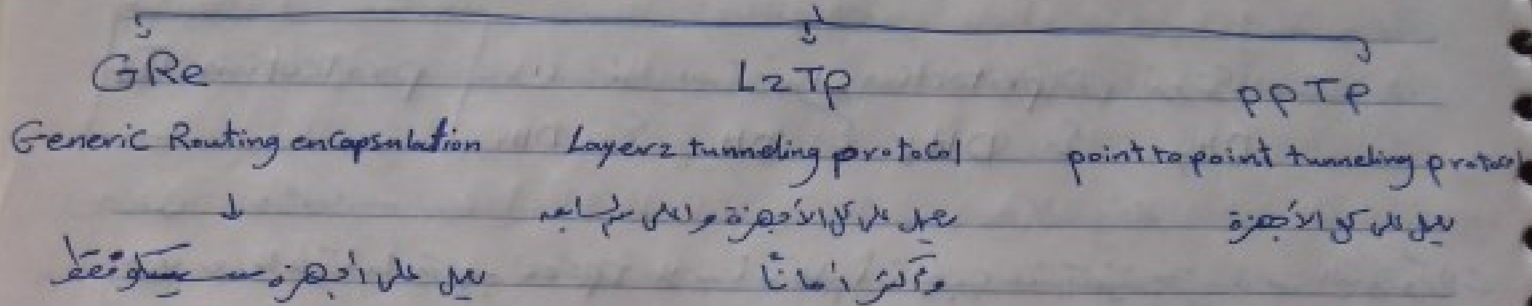
ExtraNet

ربط جميع أجهزة الكمبيوتر الخاصة بموقعين لشركات مختلفة لكن بينهم شراكة أو بين الشركة وعملائها

VPN Tunnel

فكرة الـ VPN الرئيسية هي عبارة عن بناء نفق خاص بين الجهازين أو المركز الرئيسي والفروع خلال هذا الـ Tunnel أو النفق يتم تبادل المعلومات بصورة آمنة ومشفرة. يتم امتداد هذا النفق (Tunnel) خلال الشبكة الإنترنت ليصل بين الطرفين





GRe — Generic Routing encapsulation

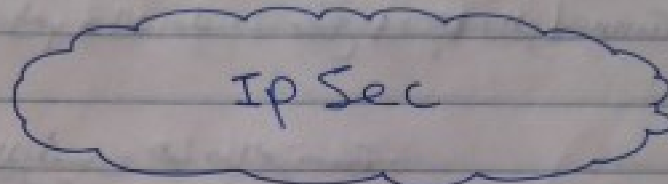
يعمل على أجهزة سيسكو فقط

L2Tp — Layer2 tunneling protocol

يعمل على كل الأجهزة والأعلى من السابقة وأكثر أمانا

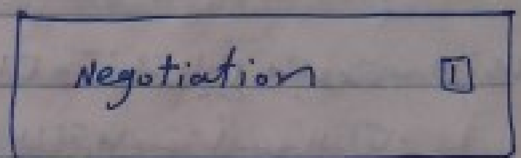
PPTP — point to point tunneling protocol

يعمل على كل الأجهزة

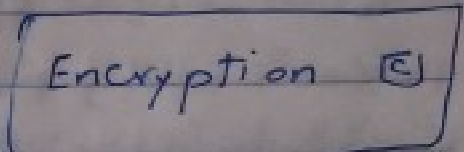


هو اختصار ← Ip Security يقوم ال Ipsec بعمل ٤ أشياء





هي عملية التفاوض التي تتم بين المركز الرئيسي والفروع والبروتوكولات المسؤولة عن عملية التفاوض هي AH و Esp و Esp+AH والأخير هو أقواهم



الداتا التي يتم إرسالها لا يتم إرسالها plain text ولكن تكون مشفرة لا يعرف محتواها إلا إذا تم فك تشفيرها والبروتوكولات المسؤولة عن عملية التشفير هي

1. Des ← Data encryption standard ← يشفر الحرف ب 56 Bit
2. 3Des ← Triple Des ← الحرف يشفر ب [3 X 56 Bit] = 168 Bit
3. Aes ← Advanced encryption standard ← يبدأ الحرف من 128 ويصل إلى 256 Bit
4. jes ← يستخدم 512 Bit لتشفير الحرف

③ Authentication المصادقة والتوثيق هل هذا المستخدم مصرح له باستخدام الـ VPN أم لا والمسئول عن عملية الـ Authentication هي بروتوكولات SHA أو MD5

④ protection والمسئول عن توفير الـ protection هي بروتوكولات DH_1 ، DH_2 ، DH_5 ، DH_7

** بعد ما عرفنا ما يقوم به Ipsec لابد أن نعلم أنه يجب عند تنفيذ حزمة من البروتوكولات في موقع [المركز الرئيسي] لابد أن نفعلها على الموقع الآخر [الفرع] حتى نقوم بإنشاء الـ Tunnel بشكل سليم وإلا فلن نستطيع إنشاء الـ Tunnel

مثال

اذا فعلنا في المركز الرئيسي هذه الحزمة.

① negotiation → Esp
② encryption → 3Des
③ Authentication → MD5
④ protection → DH_2

إذا فعلنا هذه الحزمة فلابد أن نفعلها على الطرف الآخر حتى يتم إنشاء الـ Tunnel

** عند إرسال الداتا تتم عملية encapsulation للداتا وتضاف عليها مجموعة من الإضافات تشمل الداتا المشفرة و VPN Header وغيرها. وبذلك تتم عملية تأمين الداتا.

Types of Encryption keys

ينقسم التشفير إلى نوعين ← Symmetric / Asymmetric

① Symmetric : متماثل :

كلمة السر المستخدمة في التشفير وفك التشفير واحدة ويعلمها كل من المرسل والمستقبل و يستخدم في هذا النوع Des - 56 Bit أو 3Des - 168 Bit أو Aes . 128 ، 192 ، 256 Bit

② Asymmetric غير متماثل

كلمة السر المستخدمة في التشفير غير المستخدمة في فك التشفير والمرسل والمستقبل كل منهما له كلمة سر مختلفة عن الآخر وكل منهما لا يعلم كلمة السر الخاصة بالآخر ويعتمد على نوعين من الـ Keys ١. pubic Key ٢. private Key

الـ pubic key يكون مع كل الناس والـ private key لا يعرفه إلا صاحبه فقط

(مثال) ٣ فروع A و B و C عندما يرسل A إلى B فإنه يشفرها بالـ public key الخاص بالفرع B ويرسلها يستقبلها B ويفكها بالـ private key الخاص بـ B وبالتالي لو حاول C مثلاً الحصول على الداتا هذه البيانات لا يستطيع لأنه لا يملك الـ private key الخاص بالفرع B وهكذا

ويستخدم في هذا النوع Asymmetric

- DH يبدأ 768 إلى مالا نهاية للرقم المشفر
- RSA يبدأ 512 إلى مالا نهاية الرقم المشفر

Authentication, verifing, Identifies

يتم استخدام أو تفعيل الـ Authentication بطريقتين

PKI (public key infrastructure)

باختصار يقوم هذا النوع بإنشاء ما يسمى Certificate Authority شهادة توثيقية يكون فيها اسم الراوتر والتشفير ووقت التشفير متاح لأي وقت وبيانات التشفير هذه الشهادات تعمل على توثيق كل أطراف الاتصال في الشبكة وإذا تم التوافق يتم الاتصال ولكن إذا كان هناك اختلاف لا نستطيع إنشاء الـ Tunnel

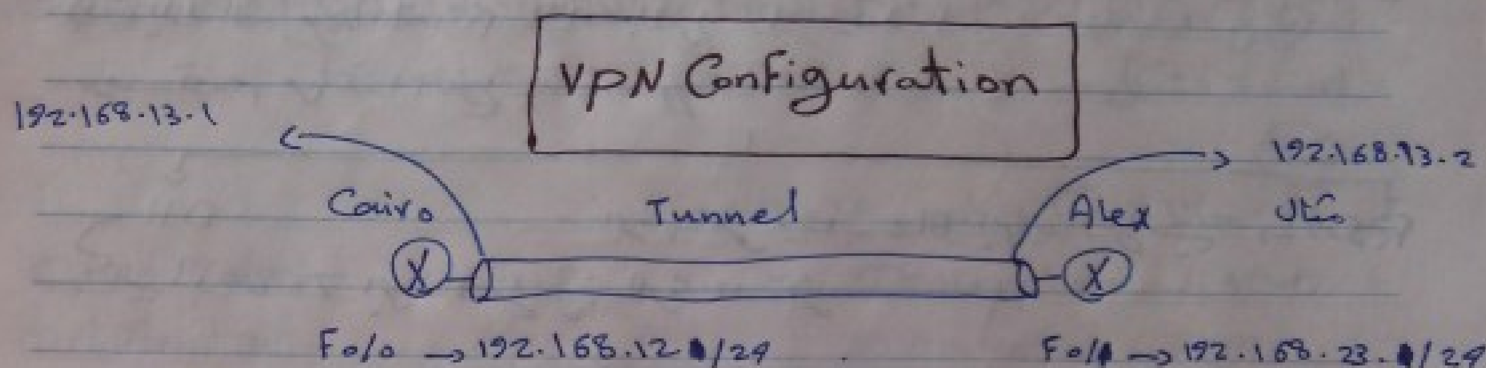
PSK (pre-shared keys)

هي عبارة عن كلمة سر واحدة يتم بها التشفير يستخدمها أحد الأطراف ويقوم الطرف الآخر بفك التشفير بنفس كلمة المرور، وعند التوافق يتم الاتصال بين الطرفين والسماح للجهاز للدخول للشبكة أو بمعنى آخر التواصل مع الطرف الآخر.

Data integrity ← هي عبارة عن سلامة البيانات من التعديل عليها ويتم ضمان ذلك عن طريق عملية تدعى Hashing للداتا حيث أن البيانات المرسلة بين الاطراف تكون مشفرة فلو استطاع احدا كان أن يحصل على نسخة من البيانات فسيجدها مشفرة فلو حاول فك تشفيرها سيغير حجم الداتا وبالتالي يكتشف الطرف الذي أرسلت إليه الداتا بأنه تم التعديل عليها وبالتالي يرفض الداتا ويتم عمل الـ Hashing للداتا عن طريق خوارزميات مثل

1. MD5 ⟶ 128 Bit
2. SHA ⟶ 160 Bit

VPN Configuration



Cairo

```
Cairo(Config)# int F0/0
Cairo(Config-if)# ip address 192.168.12.1 255.255.255.0
Cairo(config-if)# No shutdown
Cairo(Config-if)# exit
Cairo(Config)# interface tunnel 1
Cairo(Config-if)# Ip address 192.168.13.1 255.255.255.0
Cairo(Config-if)# Tunnel mode GRE ip
Cairo(Config-if)# Tunnel Source F0/0
Cairo(Config-if)# Tunnel destination 192.168.13.2
```

Alex

```
Alex(Config)# int F0/1
(config-if)# ip address 192.168.23.1 255.255.255.0
(Config-if)# No shutdown
(Config-if)# exit
(Config)# interface Tunnel 1
(Config-if)# ip address 192.168.13.2 255.255.255.0
(Config-if)# Tunnel mode gre ip
(Config-if)# Tunnel Source F0/1
(Config-if)# Tunnel destination 192.168.13.1
```

ونفعل أحد بروتوكولات الراوتنج ospf أو Eigrp.

Show Command → # Show interface Tunnel

IPv6

مقدمة: كان IPv4 يتكون من 32Bit عبارة عن 4octet حيث كل octet يتكون من 8Bits وكل octet يحتوي على رقم من صفر إلى 255 وكان عنوان الـ IPv4 يسمح لنا بإعطاء عناوين لـ 4.3 مليار جهاز تقريبًا لكن مع تطور وسائل الاتصال وانتشار ثقافة الانترنت تزايد دخول الأشخاص حول العالم بشكل كبير ما أدى إلى نفاذ تلك العناوين فكان من الواجب اكتشاف طريقة جديدة للعنونة تعطينا مساحة أكبر من العناوين مع تزايد المشتركين الذين يدخلون إلى شبكة الانترنت يوميًا. نتيجة لذلك ظهر الاصدار الجديد من بروتوكول الانترنت وهو IPv6 الذي يوفر عدد كبير جدًا من العناوين وهو ما يقارب بـ 340 تريليون تريليون تريليون عنوان وهو عدد ضخم جدًا حيث يمكن أن يكون للشخص الواحد ما يزيد على 5000 عنوان مما يحل الكثير من المشاكل التي تواجهها الشركات والتي ألجأتها لاستخدام الـ NAT والاكتفاء بعناوين داخلية خاصة مختلفة لكنها موحدة في الاتصال بالإنترنت أي تخرج للانترنت على IP عام واحد "pubic".

شكله: يتكون عنوان IPv6 من 128Bits وينقسم إلى 8 quartet ومعنى Quartet أي رباعي بمعنى أن كل quartet يحتوي على أربع أرقام سداسي عشرية (hexadecimal) وكل رقم سداسي عشري مكون أو يقابله 4Bits لذلك نجد أن كل quartet هو عبارة عن 16Bits. والأرقام السداسي عشرية هي من صفر إلى 9 ومن A إلى F بالتالي يكون شكل IPv6 كالتالي

00AB : CF00 : 2939 : 1270 : 3210 : 9210 : 5611 : 877 : 991A

يفصل بين كل quartet وآخر [:] وتسمى كولن

* عبارة عن 8quartet
* كل Quartet = 16Bits
* كل Quartet = ٤ أرقام hexadecimal وكل رقم = 4Bits
* الأرقام الـ hexadecimal هي من [0 : 9] + من [A : F]
* إجمالي IPv6 = 128Bits

* ⇐ بالفعل بدأ تطبيق IPv6 في بعض البلدان وتم إنشائه في عام ٢٠٠١م ولذلك جعلوا العناوين التي تبدأ بـ 2001 هي العناوين الـ public وسيأتي الوقت الذي يلغى فيه العمل بـ IPv4 ويستبدل كليًا للعمل بـ IPv6

★ اختصار وتبسيط عنوان IPv6 ★

لاحظنا أن عنوان IPv6 عنوان طويل حيث يتكون من 8 quartet وكل واحد منهم يتكون من أربع أرقام hexadecimal فهو عنوان طويل نسبيًا وبالتالي نحتاج التغلب على هذه المشكلة ← بالفعل تم ذلك عن طريق اختصار العنوان أو بمعنى آخر تبسيطه بعدة طرق أو بمعنى أصح طريقتين

(أ) الطريقة الأولى

- في هذه الطريقة يتم إلغاء الصفر على اليسار من الكتابة إذا كان الرقم مكون من صفر على اليسار + رقم مثل (0008) هذه نجعلها [8]
- أيضًا يتم اعتبار الـ quartet الذي كله أصفار نكتبه صفر واحد فيكون (0000) نكتبه هكذا [0]

(ب) الطريقة الثانية

- في هذه الطريقة نستخدم فكرة حذف الصفر على اليسار في الـ quartet الذي به صفر على اليسار + رقم مثل (0008) تصبح (8)
- أيضًا يتم اعتبار الـ quartets التي كلها أصفار وهم متتالية نكتب صفر واحد ثم نكتب بعدها (::) لكن نراعي أن العنوان يسمح بوجود (::) مرة واحدة فقط

(مثال)

1FE2 : 0000 : 0000 : ABCD : 0000 : 0000 : 0000 : 0058

(أ) يتم اختصار هذا الرقم كالتالي حسب الطريقة الأولى

1FE2 : 0 : 0 : ABCD : 0 : 0 : 0 : 58

(ب) يتم اختصار هذا الرقم كالتالي حسب الطريقة الثانية

1FE2 : 0 :: ABCD : 0 : 0 : 0 : 58

[أو]

1FE2 : 0 : 0 : ABCD : 0 :: 58

ونلاحظ أن [::] تكررت مرة واحدة في العنوان حيث لا يمكن أن تأتي أكثر من مرة وبالتالي الشكل التالي خطأ ←

1FE2 : 0 :: ABCD : 0 :: 58 X

خطأ لأنه كرر [::] أكثر من مرة وهي لا توجد إلا مرة واحدة فقط في العنوان

(IPv4 mask) ⟸ كما في IPv4 بأنه عن طريق الـ Subnet mask نستطيع أن نحدد الأجهزة المشتركة في الشبكة كذلك في IPv6

(مثال) حل الأسئلة التالي ⟵ 1FE2:0:0:ABCD:0::58/32
في نفس شبكة العنوان ⟵ 1FE2:0:1:2:3:4:5:6/32 أم لا.

الإجابة

أولاً نلاحظ أن الـ mask هو 32 وبالتالي نقسمه على 4Bits وهو قيمة الرقم الواحد [سداسي عشري] ∴ $\frac{32}{4} = 8$ ∴ لدينا 8 أرقام

ومعروف أن كل Quartet هو 4 أرقام ∴ 2quartet = 32 ∴ الـ Quartet الأول والثاني هما اللذان يحددان الشبكة ونجد أنهما متشابهين

1FE2 : 0 : 0 : ABCD : 0 :: 58
1FE2 : 0 : 1 : 2 : 3 : 4 : 5 : 6

وبالتالي هما من نفس الشبكة.

* جدول التحويل من hexadecimal إلى Binary والعكس

hexa	Binary	hexa	Binary
0	0000	8	1000
1	0001	9	1001
2	0010	A	1010
3	0011	B	1011
4	0100	C	1100
5	0101	D	1101
6	0110	E	1110
7	0111	F	1111

يتم التحويل من hexa إلى Binary عن طريق تحويل كل رقم وليس كل الرقم يعني 128 يتم تحويل الواحد إلى 0001 والاثنين إلى 0010 والثمانية إلى 1000

وبالتالي يكون الرقم 128 = 000100101000 في حين أنه في IPv4 = 10000000

وللتحويل من Binary نقسم الرقم إلى مجموعات كل مجموعة 4 أرقام فيكون الرقم 000100101000 = 1000 ، 0010 ، 0001 ونحول = 128

Types of Communication

1. uniCast ← هي عملية ارسال البيانات من طرف جهاز في الشبكة إلى جهاز آخر على الشبكة وفقط أي العملية تكون بين A و B فقط
وهذا النوع يستخدم في IPv4 و IPv6

2. multicast ← هي عملية ارسال البيانات من جهاز إلى مجموعة من الأجهزة وليس كل الأجهزة في الشبكة ويستخدم في IPv4 و IPv6

3. Broadcast ← هي عملية إرسال البيانات من جهاز إلى كل الأجهزة في الشبكة ويستخدم فقط في IPv4 وأما IPv6 فيستخدم anycast

4. Any Cast ← يعمل هذا النوع مع الراوتر ويقوم باختيار أقرب مسار مثلاً لو أنه سيرفرات موقع يوتيوب في المانيا وايطاليا وامريكا واليابان فإنني عند الاتصال بيوتيوب يقوم باختيار أقرب مسار وهو ايطاليا مثلاً ويعني هذا أنه كل السيرفرات مفعل عليها نفس عنوان الـ IPv6 كله مع بعض الـ Config التي تمنع تصادم الاتصالات. فتقوم فكرة الـ anycast على اختيار أقرب مسار لهذا السيرفر.

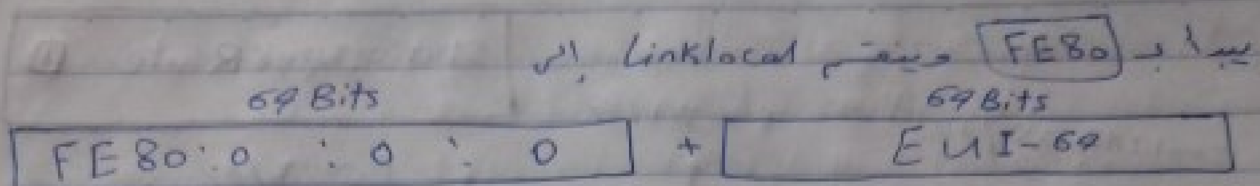
مصطلحات أخرى

1. unique local ← يقابلها في IPv4 (Local) وهي هذه العناوين التي تبدأ FD...

2. Global uniCast ← يقابلها العناوين الـ public في IPv4 وهي العناوين التي تبدأ 2000 أو 3000

3. multiCast ← تبدأ FF..

4. Link local ← وهو عبارة عن العنوان الذي يأخذه الجهاز بشكل افتراضي في حالة IPv4 في حالة إذا لم نعطي الجهاز عنوانه بشكل يدوي وأيضاً لم يأخذ عنوانه عن طريق سيرفر DHCP فيأخذ عنوانه يسمى ApipA ويكون كالتالي 169.254.X.Y والذي يقابله في IPv6 هو العنوان الذي



FE80:0 : 0 : 0 + EUI-64

حيث أن ⇐ EUI يتم احتسابها كالتالي

EUI = Frist half of mac + FFFE + end half of mac

مثال لو عنوان الماك هو 1612-3956.789A

يكون الـ EUI هو 1612.39FF.FE56.789A

ويكون عنوان الـ Linklocal لهذا الجهاز هو

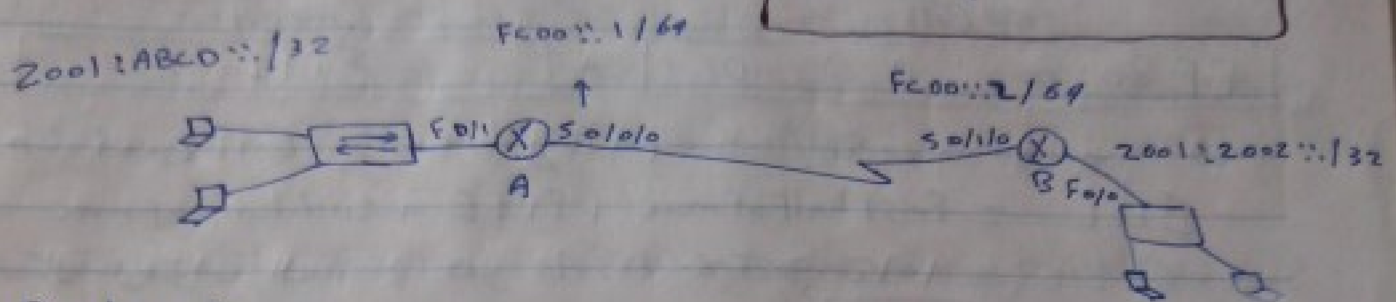
FE80:0:0:0:1612.39FF.FE56.789A

★ عنوان الـ linklocal هنا هو البديل الاعتماد عليه في IPv6 حيث في IPv6 لا يوجد بروتوكول ARP الذي كانت وظيفته معرفة عناوين الماك للأجهزة المتصل في الشبكة حيث في IPv6 يتم استخدام NDP ← Neighbor Discovery protocol الذي يستخدم عناوين الـ Linklocal مكان الـ mac أي بدلاً منها

Ipv6 MultiCast Addresses

1. FF02::1 → كل الأجهزة على اللينك التي تستخدم IPv6
2. FF02::2 → كل أجهزة الراوتر على اللينك
3. FF02:5 → يستخدمه بروتوكول ospf
4. FF02:6 → يستخدمه ospf للإرسال إلى DR
5. FF02::A → يستخدمه بروتوكول Eigrp

Ipv6 Routing Configuration



① Router A

Router>en

Router#Config t

Router(Config)# int serial0/0/0

Router(Config-if)# Ipv6 address FC00::1/64

Router (Config-if)# No shutdown

Router(Config-if)# int F0/1

Router(config-if)# ipv6 address 2001:ABCD::1/32

Router(config-if)# No shutdown

☆ الآن تعريف الشبكة التي ستتصل بـ static

Router(Config)# ipv6 Route 2001:2002::/32 S0/0/0

أو Router(Config)#ipv6 Route 2001:2002::/32 FC00::1/64

أو Router(Config)# ipv6 Route 2001:2002::/32 FC00::2/64

---

② Router B ←

نعطي الانترفيس العناوين الخاصة به كما فعلنا في راوتر A

☆ الآن عمل الـ StaticRoute

Router(Config)# Ipv6 Route 2001:ABCD::/32 S0/1/0

أو Router(Config)# Ipv6 Route 2001:ABCD::/32 FC00::2/64

Router(Config)# Ipv6 Route 2001:ABCD::/32 FC00::1/64

Router# Show Ipv6 Route Static

2 Default Route

في المثال السابق لو أردنا تفعيل ال Default route ومعناه العنوان بأي Subnetmask

Router A

Router(config) # Ipv6 Route ::/0 Serial 0/0/0

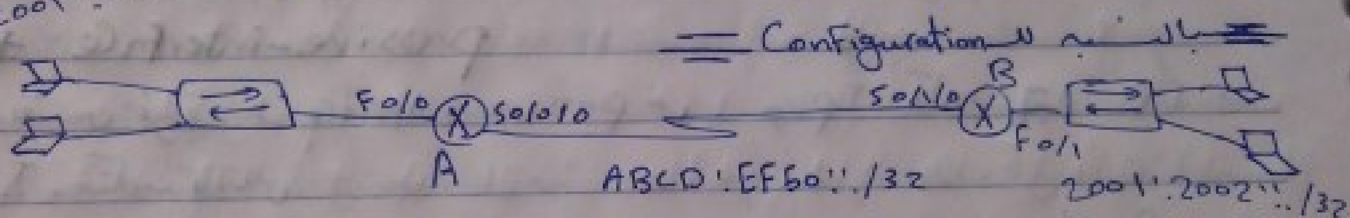
Router B

Router(Config) # Ipv6 Router ::/0 Serial 0/1/0

3 OSPF v_3

OSPF v_3 ⇐ هو الاصدار من بروتوكول OSPF الذي يعمل مع IPv6 وإذا كان OSPF v_2 يستخدم العنوان 224.0.0.6 كعنوان DR/BDR وكذلك عنوان 224.0.0.5 للـ multicast فإن OSPF v_3 يستخدم FF02::6 كعنوان DR/BDR وكذلك العنوان FF02::5 للـ multicast

بالنسبة للـ Configuration



Router A

Router(config) # Ipv6 uniCast-Routing

Router(Config) # Ipv6 Router ospf 40 ⟵ process id

Router(config-rtr) # Router-id 1.1.1.1 ⟵ نفس الروتر id على شكل IPv4

Router(config-rtr) # exit

Router(Config) # int S0/0/0 — ندخل على الانترفيس

Router(config-if) # Ipv6 OSPF 40 area 0

(40: كا رقم العملية — 0: رقم ال Area)

Router(Config) # int F0/0

Router(config-if) # Ipv6 ospf 40 area 0

Router B

```
Router(config)# Ipv6 unicast-Routing
Router(config)# Ipv6 Router ospf 50        مثلا
Router(config-rtr)# Router-id 2.2.2.2
Router(config-rtr)# exit
Router(config)# int S0/1/0
Router(config-if)# Ipv6 ospf 50 area 0
Router(config)# int F0/1
Router(config-if)# Ipv6 ospf 50 area 0
```

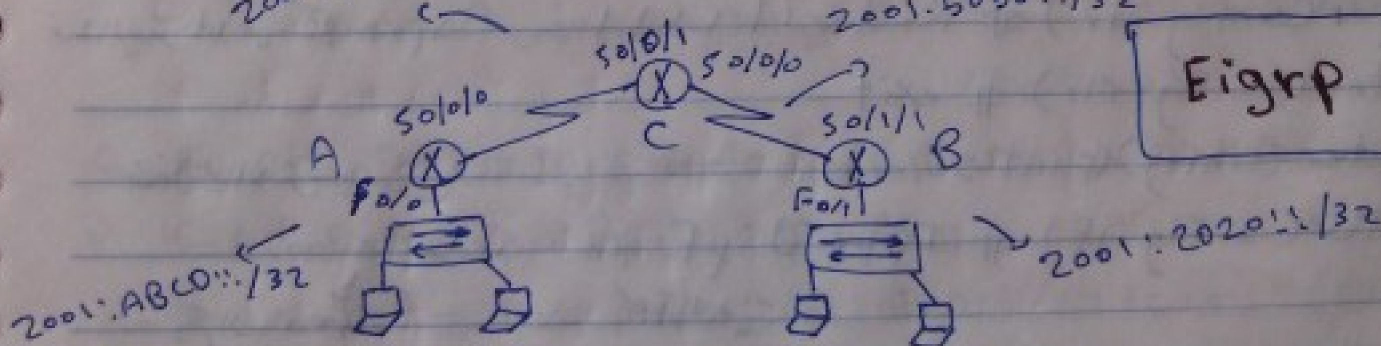
#Show Ipv6 Route — #Show ipv6 ospf
#Show ipv6 protocols — #Show Ipv6 ospf interface
#Show ipv6 interface brief — #Show ipv6 ospf neighbor
#Show ipv6 ospf Database — #Show Ipv6 Route ospf

passive-interface *

هي نفس طريقة ال passive-interface في Ipv4 لكن نستبدل IP ب Ipv6 فتكون كالتالي

```
Router(config)# Ipv6 Router ospf 50        مثلا
Router(config-rtr)# passive-interface F0/0        مثلا
```

* نستطيع تفعيل اي أمر كنا نستخدمه في Ipv4



9- Eigrp

Router A

Router(config) # Ipv6 unicast-routing

Router(config) # Ipv6 router eigrp 5

Router(config) # Noshutdown

Router(config-rtr) # router-id 1.1.1.1

Router(config-rtr) # exit

Router((config) # int F0/0

Router(config-if) # Ipv6 eigrp 5

Router(config-if) # int S0/0/0

Router(config-if) # ipv6 eigrp 5

ونتبع نفس الخطوات على راوتر B ؟

وبالنسبة لأوامر ال Show

#Show ipv6 eigrp interface

#show ipv6 eigrp neighbor

#Show Ipv6 Route

#Show ipv6 protocols

#Show ipv6 eigrp Topology

#Show ipv6 ~~eigrp~~ route eigrp

Network management

NTP ①

هو اختصار Network time protocol وهو بروتوكول وظيفته ضبط الوقت على أجهزة الشبكة بطريقة أوتوماتيكية

بحيث تكون أجهزة الشبكة جميعها لها نفس الوقت والتاريخ

فكرة عمله

فكرة عمله عبارة عن سيرفر تم ضبط الوقت والتاريخ عليه وتقوم أجهزة الشبكة بالحصول على الوقت والتاريخ عن طريق الاتصال بهذا السيرفر. مع العلم انني أستطيع أيضاً ضبط الساعة أيضاً على الأجهزة بشكل يدوي

① ضبط الساعة يدوياً.

```
Router # clock set 08:05:17 29 mar 2019
```

نلاحظ اننا كتبنا الامر على الـ priviledge وبدانا بالساعة ثم الدقائق ثم الثوان ثم كتبنا التاريخ اليوم ثم الشهر ثم السنة

② ضبط سيرفر NTP

* السيرفر سيكون مفعل عليه الوقت والتاريخ المراد نقله لكل أجهزة الشبكة
* نقوم بإعطاء السيرفر IP وهو الذي سيعرف الأجهزة التي ستحصل على الوقت والتاريخ منه السيرفر أنه هو السيرفر

```
Router > en
Router # Config t
Router (config) # NTP server { server IP }
Router # show nTP status
Router # show nTP associations.
```

* يساعد بروتوكول NTP في عمليات إدارة ومراقبة للشبكة.

٤ DNS

Dns ← هي اختصار Domain name system وهي خدمة أو بروتوكول يقوم بتحويل وترجمة أسماء المواقع إلى ايبهات.

في البداية يجب أن نعلم أن أسماء المواقع مثل yahoo.com ، google.com وغيرها من المواقع هي في الحقيقة أسماء وهمية وجدت لتسهيل التصفح للمستخدم هذه الأسماء هي في الأساس عناوين Ip.

مثلاً ← موقع google.com عنوان الـ Ip الخاص به هو 173.194.35.18 فإذا كتبنا في المتصفح google.com أو 173.194.35.18 فإن النتيجة النهائية واحدة وهي موقع google.com ، لذلك إذا كتبنا الاسم فإن بروتوكول الـ Dns يقوم بترجمة هذا الاسم إلى عنوان Ip

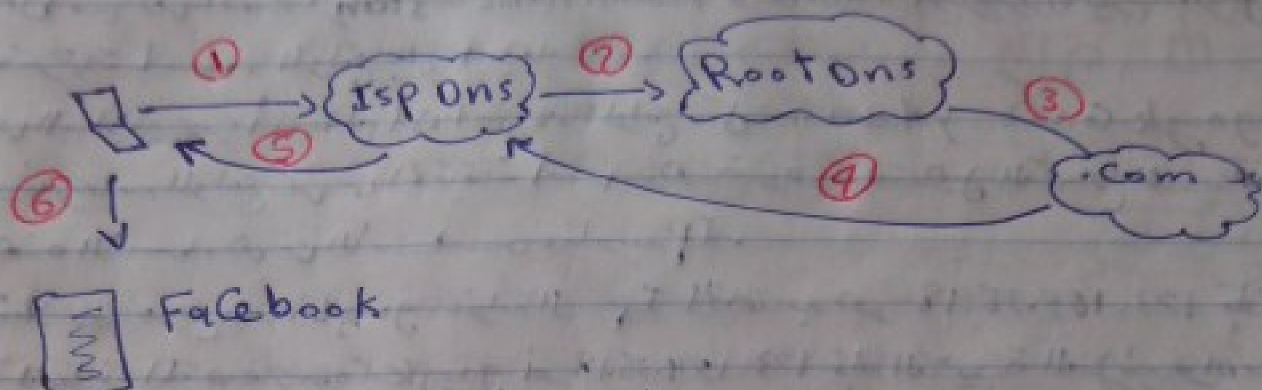
فائدته ← فائدة Dns كبيرة جداً حيث لا يستطيع المستخدم حفظ عنوان الـ Ip الخاص بكل موقع في حسبانه يسهل عليه حفظ اسم الموقع ويقوم بروتوكول الـ Dns بتحويل هذا الاسم إلى عنوان Ip

فكرة عمله ←

يقوم المستخدم [client] بمحاولة الاتصال بموقع وليكن مثلاً Facebook.com أول مرة يتصل فيها يكون الجهاز [client] لا يعرف ما هو الـ Ip الخاص بـ Facebook وبالتالي يتصل بـ Dns سيرفر الذي تقدمه شركة Isp المزودة لخدمة الانترنت الذي يقوم بترجمة الاسم لعنوان Ip ويرد على الـ client بالعنوان فيقوم الـ client بالاتصال بنجاح بموقع Facebook

* بفرض أن Dns سيرفر الذي عند Isp لا يوجد عليه Ip عنوان موقع معين فإن أي Dns سيرفر الخاص بـ Isp يتصل بـ Dns Root وهو عبارة عن سيرفرات مسجل عليها جميع مواقع الانترنت مثل com. ، net. ، org. edu. وهكذا فيعرف DnsRoot عن طريق الاسم المرسل إليه هل هو خاص بموقع تبع com. أو net. وهكذا وبالتالي لو com. يحول الاستفسار إلى سيرفر الـ Dns الخاص بمواقع الشركات com. والتي يكون مسجل عليها أسماء المواقع

التي تنتهي بـ com. وبالتالي يرسل عنوان الـ ip لـ الـ Dns سيرفر الموجود في شركة isp والذي يرسل العنوان ip للـ client



* بالطبع لن يحدث ذلك في كل مرة يحاول فيها الـ client الاتصال بموقع ما لكن يحدث في حالة إذا لم يكن الـ client زار الموقع قبل هذا الوقت وطالما قد زاره فإنه يتم تسجيله عنده وكذلك في Dns isp وبالتالي لن تتكرر العملية

* يستخدم Dns أيضاً في الشركات حيث تقوم كل شركة بتسجيل قائمة بأسماء الأجهزة أو الأشخاص بدلاً من الاتصال عن طريق الـ ip فإذا أرادت الشركة أن يكون العنوان 192.168.10.1 هو عنوان المدير مثلاً manager1 فإنه يتم تسجيله على سيرفر الـ Dns وهكذا ما يسهل عملية الاتصال حيث أنني أتذكر الاسم ويصعب علي تذكر عنوان ip الخاص بجهاز المدير وهكذا.

مكونات الـ Dns

① Resource Records ⟶
هي بيانات المواقع والايبهات الخاصة بها وتكون مسجلة على أكثر من سيرفر

② Dns name server ⟶
وهو السيرفر Dns ويكون مسجل عليه المواقع وأيبهاتها ولديه امكانية الاجابة على استفسارات الـ client وكذلك الارسال للسيرفرات الأخرى لتعلم الـ Records التي ليست موجودة لديه

③ Dns Resolver ⟶
وهي الخاصية في الـ client والسيرفر التي تتيح الاستفسار عن الـ Records الغير مسجلة لديهم.

SysLoG ③

هي اختصار System Logging وهي خدمة تسمح للأجهزة بـ... الخدمة وأيضا بعض الأجهزة الأخرى المرتبطة بالشبكة بإرسال الرسائل التي تظهر على شاشة التشغيل عبر الشبكة إلى سيرفرات خاصة ليتم مراجعة هذه الرسائل ومعرفة من كان له login وما هي الأوامر التي تم تنفيذها على أجهزة الشبكة سواء الراوتر أو سويتش

(مثال)

عندما نكتب أمر على الانترفيس بجعلها down فإننا ندخل على الانترفيس ونكتب الأمر shutdown ستظهر لنا رسالة

F 0/0 changed state to down

أي تم تغيير حالة الانترفيس من up إلى down وسيتم إرسال هذه الرسالة إلى السيرفر الذي خصصناه مسبقا ليتم حفظ مثل تلك الرسائل عليه لنقوم بمراجعتها في أي وقت شئنا

(فائدته) هذه الخدمة أو البروتوكول يتيح لنا عملية monitoring أو مراقبة للشبكة بمعنى طريقة نستطيع معرفة من دخل إلى اعدادات الراوتر والسويتش وما هي الأوامر التي تم تطبيقها على الشبكة. وذلك أيضا يفيدنا في عملية الـ Troubleshooting لحل مشاكل الشبكة.

* هذه الرسائل يمكن أيضا أن تحفظ داخل الـ RAM وتسمى الـ Logging buffer ولكن هذه تفقد في حالة إيقاف تشغيل الراوتر أو السويتش.

شكل الرسالة

*Dec 18 17:10:15.079 ; 0/0 lineproto-5-updown: Line protocol on interfa(c)e Fastethernet 0/0, changed state to down

تنقسم هذه الرسالة إلى عدة أشياء

① الوقت ← يمثله الجزء Dec 18 17:10:15.079 .

② المرفق الذي عمله أنشأ الرسالة ← ويمثله 0/0 lineproto

③ مستوى الخطورة [The severity Level] ← 5

④ تذكير الرسالة بـ ← updown

⑤ وصف الرسالة ← الخ lineprotocol on interface ________

Severity level

هي مستويات الخطورة بالنسبة للرسالة حيث يوجد مستويات من الخطورة هي كالتالي

level	level name	
0	Emergency	تكون النظام غير قابل للاستخدام
1	Alert	يكون هناك حاجة لإجراءات فورية
2	Critical	وقوع أو حدوث حدث خطير
3	Error	رسالة خطأ
4	Warning	حالة تستدعي التحذير
5	Notification	رسالة تنبيه لأمر هام
6	Informational	اعلام بأمر طبيعي
7	Debugging	الامر هو عبارة عن ناتج أمر لتصحيح خطأ سابق

* يستطيع الادمن تحديد ما هي الرسائل التي سيرسلها الراوتر أو السويتش إلى سيرفر الـ syslog سواء كلها أو بعضها.

كيفية اعداد الـ syslog

① كما لاحظنا هو سيرفر يتم ارسال هذه الرسائل عليه وبالتالي لابد أن يكون لدينا جهاز سيرفر ذو IP معلوم

② برنامج يكون موجود لدى الأدمن يمكنه من قراءة ومتابعة هذه الرسائل المرسلة من الراوتر والسويتش مثل برنامج Kiwi syslog أو TFtp

③ تفعيل الاوامر الخاصة بـ syslog على الراوتر أو السويتش المراد مراقبة ما تم عليه من اجراءات.

مثال السيرفر هو 192.168.10.1

Router >en
Router # Config t
Router(config) # logging 192.168.10.1

هذا الامر يتم ارسال الرسائل للسيرفر 192.168.10.1

* يمكننا التحكم في استقبال الرسائل بطريقة محددة مثل أن نحدد مستويات الخطورة من 0 إلى 4

Router(config) # Logging 192.168.10.1
Router (config) # Logging Trap 4 (0 : 4)

* أو نحدد نوع واحد فقط من الرسائل ولكن هذا يكون عن طريق كتابة نوع الرسالة مثل التحذير مثلاً نكتب warning

Router (config) # Logging 192.168.10.1
Router (Config) # Logging Trap warning

Modifying system Messages #

التعديل على الرسائل يتيح لي أن أعدل الرسائل بحيث تظهر لي بأرقام متسلسلة بدلاً من الظهور بطريقة مؤرخة ولتفعيل ذلك نتبع الآتي

Router(config) # No service timestamps.
Router(config) # service Sequnce-numbers

ولكن التاريخ أفضل في عملية المراقبة حيث أستطيع معرفة تاريخ الأوامر وهكذا تكون المراقبة أفضل ولإرجاع التاريخ نعكس العملية السابقة

Router (config) # No service Sequnce-numbers
Router(config) # Service Timestamps.

أوامر Show

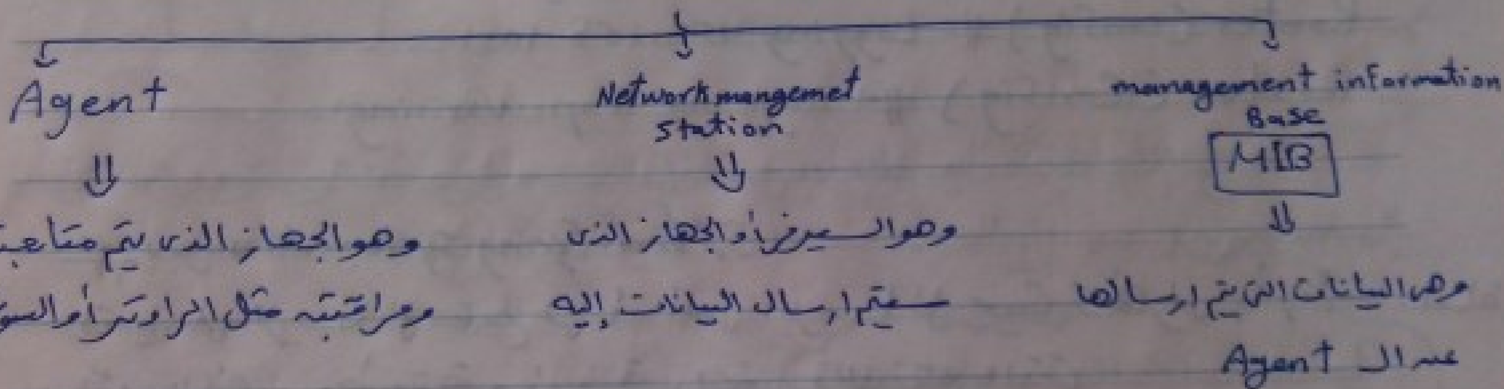
Router # Show logging

SNMP -9

هي اختصار ⇐ Simple network Management protocol وهو عبارة عن بروتوكول يتيح لنا مراقبة الشبكة و يستطيع العمل مع جميع مكونات الشبكة من راوتر وسويتش وطابعة ومثلا نستطيع من خلاله مراقبة معدل استهلاك الباندويدث ومعدل استهلاك الـ cpu البروسيسور - فترة عمل الجهاز - ومتى تم اطفاء الجهاز ومتى تم إعادة تشغيله وكذلك متابعة الـ Traffic هل هو HTTP أو HTTPs أو FTP أو أي شيء آخر

Snmp Components

يتكون الـ Snmp من ثلاثة أشياء

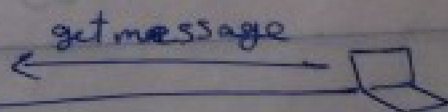


Snmp message

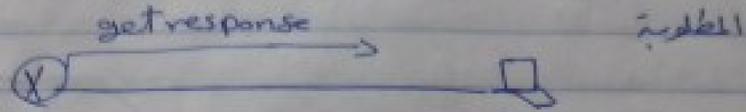
تنقسم رسائل بروتوكول Snmp إلى ثلاثة أنواع

① رسائل get ⇐ وهي الأكثر استخداما وتنقسم إلى getmessage وإلى getresponse

* عندما يريد السيرفر من الـ Agent أن يرسل إليه البيانات يرسل له رسائل الـ getmessage

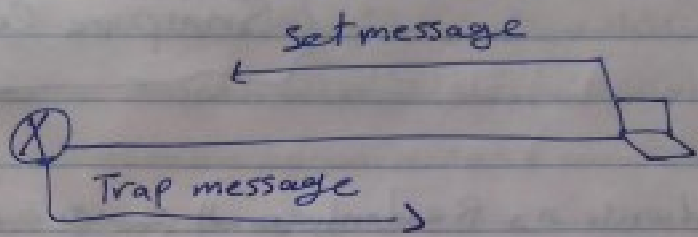


• getresponse ← هي الرسائل التي يرسلها الـ Agent للسيرفر بالبيانات المطلوبة

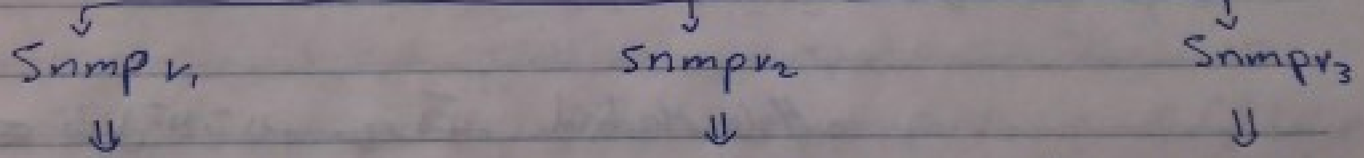


② رسائل الـ set ← هي نوع آخر من رسائل snmp وهي الرسائل التي يرسلها السيرفر للـ Agent يأمره ببعض الأوامر وهذا النوع من الرسائل نادر الاستخدام . وهي الرسائل بمعنى أرسل لي بيانات إذا حدث شيء معين تحدده

③ رسائل الـ Trap ⟸ هي نوع آخر من الرسائل يرسلها الـ Agent للسيرفر كشكوى عند حدوث الشيء الذي تم تحديده مسبقًا



إصدارات snmp



- Snmp v1 ⇓ يستطيع رصد البيانات حتى ١٠٠ ميجا وهو غير آمن حيث كلمة السر التي يتم تفعيلها على الراوتر والسيرفر تكون clear text
- Snmp v2 ⇓ يستطيع رصد حتى ١٠ جيجا من البيانات ولكنه أيضًا غير آمن حيث الـ password فيه clear text
- Snmp v3 ⇓ عالي الأمان حيث يستطيع عمل Hashing وتشفير للداتا encryption

Snmp v2

بالنسبة لهذا الإصدار، فإنه يوفر نوعين من الاتصال

- readonly – Ro: حيث يسمح بقراءة البيانات المرسلة فقط دون التعديل عليها
- Rw: يسمح بالقراءة والتعديل على البيانات

وبما أنه V2 من الـ Snmp هو غير آمن فإن الشركات التي تخصه تجعله read only

Snmp V3

الإصدار الثالث هو أفضل إصدار حيث فيه إمكانية تشفير الداتا و عمل مصادقة وهاشينج للداتا و مع أنه في بعض المستويات الخاصة به حيث فيه أكثر من level في بعضها لا يوجد بعض تشفير إلا أنه أفضل من V2 حيث مازال بـ Authentication و Data integrity

Snmp v2 Configurations.

إعدادات خاصة بعمل الـ Readonly والـ Readwrite

⟸ إنشاء الـ Acl بالأجهزة المسموح لها استقبال البيانات من الأجهزة المراقبة

```
Router(config) # ip access-list standard MeMo
Router(config-std) # permit host 10.10.10.101
Router(config-std-nacl) exit
```

⟸ تفعيل كلمة السر و لتكن Hala Madrid

```
Router(config)# Snmp-server Community halamadrid Ro MeMo
                                                 Rw
```

- halamadrid ← كلمة السر
- Ro ← الإذن الذي يحدد عمل الـ Readonly
- لو أردنا Rw
- MeMo ← اسم الـ Acl

⟸ تحديد ما سيتم مراقبته

```
Router(Config) # Snmp-server enable Traps ?
```

ومن علامة الاستفهام سيظهر لنا ما يمكن مراقبته نختار ما نريد مثل

```
Router(config) # Snmp-Server enable Traps snmp linkup Linkdown
```

وبعض الاوامر الاختيارية مثل مكان السيرفر و الاتصال بالمسئول عن المراقبة وبعض التفاصيل

```
Router(config)#snmp-server Contact Ahmed Habib -network admin
Router(config)#snmp-server location _ _ في عنوان معين ______
```

وهكذا

NetFlow 5

هو بروتوكول شبيه بـ snmp ووظيفته مراقبة الشبكة والأجهزة من خلال تحليل الترافيك ومراقبة الباندويث في الشبكة والذي يساعدنا في رفع أداء الشبكة وهذا البروتوكول ليس حصراً على أجهزة سيسكو فقط ولكنه مدعوم من شركات أخرى لكن بمسميات مختلفة وهذه بعض الأمثلة

jFlow أو cFlowd ⟶ junipernetworks
Netstream For ⟶ Hmawi Technology
cFlowd For ⟶ Alcatel-Lucent

وغيرها من الشركات

* ويختلف snmp بأن Net flow يستطيع أن يقدم لنا تحليل ومتابعة الترافيك من خلال تحديد منفذ معين مثلاً أو من خلال IP معين وهذا كله يتم من خلال الإعدادات التي نقوم بها
* بينما نجد بأن snmp يقوم بجمع احصاءات أكثر عن الجهاز نفسه مثل الـ Traffic و platform و resource utilization وهذا يشمل احصاءات عن المعالج والرامات والأخطاء التي حدثت على الجهاز أما الـ Net flow فهو يقوم بجمع معلومات مفصلة حول الترافيك الذي يمر عبر هذا الجهاز

* يستطيع الـ Net flow جمع معلومات عن

Source Ip ، Destination Ip ، Source port ، Destination port
Ip protocols ، interface ، Ip Type of Service.

* بعد جمع المعلومات يقوم البروتوكول بتخزينها على ال Flow cache ليتم دفعها فيما بعد
أو يتم حذفها في حالة انتهاء الزمن المسموح ببقائها NetFlow Analyzer

NetFlow Configuration

① تحديد البورت الذي سنراقبه ونفعل ال NetFlow

```
Router(config)# int f 0/0
Router(config-if)# ip route cacheflow
```

② نحدد هل سيتم مراقبة الداخل أو الخارج

```
Router(config-if)# ip flow egress      البيانات الخارجة
Router(config-if)# ip flow ingress     البيانات الداخلة
```

③ نحدد الاصدار من NetFlow

```
Router(config)# ip flow-export version 5  أو 9
8
```

④ تحديد ال source وال Destination

```
Router(config)# ip flow-export source loopback 0
Router(config)# ip flow-export Destination _   الجهاز الذي نرسل إليه الداتا
```

⑤ نحدد وقت حفظ البيانات في Flow cache

```
Router(config)# ip flow-cache timeout active 1
```

أي ابدأ أرسل الاحصائيات كل دقيقة وطبعا نغيرها حسب اختيارنا

```
Router(config)# ip flow-cache timeout inactive 15
```

أي اعتبر الاتصال منقطع إذا لم تستلم أي معلومات خلال ١٥ دقيقة.

أوامر ال Show

```
Router# show ip cache flow
        show ip cache verbose flow.
```

Managing IOS

ابتداءً يتكون الراوتر أو السويتش من الآتي

Cpu ← وحدة المعالجة المركزية

RAM ← الرام وهي التي تحتوي على الإعدادات العاملة على الراوتر وتفقد محتوياتها بانقطاع التيار الكهربي

ROM تحتوي على برنامج فحص المعدات الذي يكون في بداية تشغيل الراوتر وتحتوي على برنامج Bootstrap المسئول عن ضمان تشغيل الراوتر بشكل سليم

NVRAM وهي نوع من أنواع الرام RAM إلا أنها لا تفقد محتوياتها بانقطاع التيار الكهربائي وتحتوي على الإعدادات المخزنة [إعدادات بدء التشغيل] وهي التي تنسخ إعدادات الـ RAM إليها لكي لا تفقد تلك الإعدادات عند انقطاع التيار الكهربي

Flash ← ذاكرة دائمة وتستخدم لحفظ وتخزين ملف نظام التشغيل IOS

ports منافذ الـ LAN والـ WAN ، Console ، Aux

خطوات إقلاع الجهاز

يمر الراوتر بعدة مراحل عند عملية تشغيله [إقلاع الراوتر أو السويتش]

① post ⇐ هي اختصار power on self test وهي عبارة عن عملية فحص داخلي للتأكد من سلامة أجزاء الجهاز [راوتر أو سويتش] وهل هو يعمل بشكل سليم أو به مشاكل

② Bootstrap ← بداية كل نظام تشغيل يلك نوعين من الملفات ملفات الإقلاع وملفات النظام بداية يتم تحميل ملفات الإقلاع ثم تقوم ملفات الإقلاع بتحميل ملفات النظام

Bootstrap هو الذي يقوم بعملية تحميل ملفات الإقلاع خصوصاً مسار ملفات الإقلاع وهي Ios في ال Flash أي أنه يذهب إلى ال Flash ويبحث عن ملف Ios ويكون مضغوط فيقوم بفك الضغط وتصحيح الفيروسات ثم يرسله إلى Ram ثم يذهب أيضاً إلى NVRAM ويأخذ ملف startup Config ويرسله إلى RAm

* عند عملية الإقلاع يختار Bootstrap ملف يسمى 0x2102 وهو الملف الطبيعي أي هو الذي يعني أنه تم عملية الإقلاع بصورة طبيعية
* إذا لم يجد Bootstrap ملف الإقلاع [Ios] في ذاكرة الفلاش Flash فإنه يبحث عن ملف Ios في TFTp server

③ المرحلة الثالثة هي إيجاد وتطبيق ملف الإعدادات المخزنة [إعدادات بدء التشغيل]
* يبحث في NVRAm فإنه لم يجد إعدادات
* يبحث في TFTp server فإنه لم يجد الإعدادات
* يدخل في وضع الإعدادات ويتم إدخالها عن طريق الكمبيوتر باستخدام كابل Console

Router Backsup and Restore

① Backsup Ios

من أجل عمل نسخ احتياطية من كل إعدادات الراوتر أو السويتش وأيضاً نسخ احتياطية من ملف التشغيل Ios فإننا نستخدم برنامج TFTp أو غيره من البرامج لكن TFTp أثبت كفاءته وهو صغير الحجم

* تحميل Ios من على جهاز الكمبيوتر

R # Copy Flash TFTp

IP

بعد الضغط على الأمر سيطلب اسم الفلاش & اسم السيرفر وهل تريد نسخه بنفس الاسم أو باسم آخر ثم نضغط enter سيقوم الجهاز بعملية النسخ وسنجد الملف في الجهاز الكمبيوتر في المجلد الذي حددناه مسبقاً

سيكون اجمالي الامر كالتالي

R # Copy Flash TFTp + enter

ثم سيطلب اسم أو رقم IP السيرفر فنكتبه وسيظهر لك source Filename الـ وهو اسم الملف المراد تصديره وسيظهر لك هل تريد الحفظ بنفس الاسم (نعم) # بعدها سينتقل الملف للمسار المحدد. ويكون ملف IOS امتداده هو .bin

Restor IOS

استعادة الملف من السيرفر TFTP

R # Copy TFTp Flash

سوف يسألنا عن IP السيرفر نكتبه ثم نكتب اسم ملف IOS مع امتداد الملف وعندها تبدأ عملية الاستعادة بعد الضغط على enter

* بالنسبة لأوامر الـ show

#Show Flash #Show version

R# delete Flash: ...bin لمسح الفلاش.

Backup Run / Start

R # Copy Run TFTP

ونحدد IP السيرفر واسم الملف + enter

R # Copy start TFTP

ونحدد IP للسيرفر واسم الملف + enter

بذلك تكون عملنا Backup للإعدادات.

R # Copy TFTP Run
R # Cop TFTP start

Restor Run / start

وتحدد ip السيرفر واسم الملف وبالطبع سنكتبه ثم ضغط enter وبالتالي تبدأ عملية الاستعادة.

password Recovery

بالطبع كإجراء لتأمين الشبكة يلجأ الأدمن إلى وضع password للراوتر أو السويتش لا يعرفه إلا هو أو المخول له استخدام أو إدارة الشبكة لكن ماذا لو فقدنا كلمة السر عن طريق النسيان أو الضياع أو لأي سبب آخر هنا نلجأ إلى عملية ⟸ password Recovery

بداية عملية الإقلاع الطبيعية بعد الـ post مرحلة الـ Bootstrap وفيها نذهب لملفات الإقلاع في Bootstrap عملية Ios في Flash تختار ملف معين هو المسئول عن عملية الإقلاع الطبيعية وهو 0X2102 وهنا هو الـ default والـ 0X2102 عبارة عن رقم سداسي عشري

(المهم) أن Bootstrap يختار هذا الملف 0X1202 ويقلع الجهاز بصورة طبيعية محملاً بالإعدادات السابقة التي تحمل عليها من NVRAM وبالطبع من ضمن هذه الإعدادات الإعدادات الخاصة بـ password

ما نقوم به في عملية الـ password recovery هي جعل الراوتر أو السويتش في عملية الإقلاع يقلع لكن دون أن يأخذ الإعدادات الخاصة بالراوتر على NVRAM أي أثناء الإقلاع نتجاهل NVRAM وبالتالي نستطيع الإقلاع بالراوتر دون طلب الباسورد وبالتالي يمكننا أن نحذف الإعدادات السابقة بما فيها الباسورد أو نحذف إعدادات الباسورد فقط ولكي نستطيع فعل ذلك فإننا نجعل الراوتر يختار الملف 0X2142 بدلاً

من 2102 الـ default
عن طريق هذه الخطوه نستطيع تجاوز الـ NVRAM وبالتالي نتجاوز الـ password

• طبقا بعد ادخال 0X2142 سنعمل على وضع setup config والتي من خلاله نعمل الاوامر التي من خلالها نمنح اعدادات الراوتر.

س : لماذا 0X2142 ؟
وضحنا أن الملف الـ default هو 0X2102 ووضحنا أيضا انه رقم hexadecimal وبالتالي تحويله كالاتي

hexa	0X	2	1	0	2
Binary	0X	0010	0001	0000	0010
		١٥١٤١٣١٢	١١١٠٩٨	٧٦٥٤	٣٢١٠

وهو عبارة عن ١٦ بت [16 Bits]
كل Bit له وظيفة ووظيفة الـ Bit السادس وهو NVRAM
كل ما يهمنا هو الـ Bit السادس الخاص بـ NVRAM ونلاحظ أنه في الملف الـ default قيمة Binary = صفر لكن إذا جعلنا قيمة البت السادس واحد في الـ Binary سيصبح الملف كالتالي

0X 0010 0001 0100 0010

نلاحظ البت السادس أصبح واحد وليس صفر ونقوم بتحويله من Binary لـ hexadecimal

0X 2 1 4 2

وهو الملف [0X2142]

الاعدادات :

بداية نشغل الراوتر وأثناء الاقلاع وعند ظهور الهاشتاج #### نضغط على الزر Ctrl + Pause Break ستظهر لي شاشة الـ common وبعدها نبدأ نكتب الاوامر التالية

Rommon1> Config 0x2142

بعدها نطفئ الراوتر ونشغله أو نكتب الامر

Rommon1> reset

سيعمل الراوتر ريستارت وعند التشغيل سيسأل هل تريد setup مود
نختار No ومن التالي سيفتح الراوتر على الاوامر

Router> en

Router # Copy ~~Run Start~~ Start Run

وبعدها ندخل على الجلوبال مود ونغير ال password

Router# Config t

Router(config) # enable secret AAA

وبعدها نرجع لاستخدام الملف 0x2102

Router(config)-Register 0x2102

ونحفظ العمل

Router# wr or Copy Run start

وبعدها أمر Reload لتشغيل التغييرات

Router #Reload

Erase startup Config

1 إذا أردنا أن نرجع الراوتر لحالته الاصلية ونمسح من عليه الاعدادات فإننا نتبع الآتي

Router # Write erase

ونعمل بعدها Confirm ونضغط OK. enter

وبعد التأكيد نكتب الأمر Reload

Router # reload

وسيسأل الراوتر عند الاقلاع هل تريد حفظ الاعدادات قبل إعادة الاقلاع نختار No. ونضغط enter

(ج) بالنسبة للسويتش نفس الامر بس هنضيف أمر لالغاء vlan

Switch # write erase

Switch # delete vlan.dat → الملف الخاص بـ vlan

Switch # Reload

وطبعا نأكد على ال Confirm اللي طلب مني فورد

أو ممكن نستخدم أمر مسح NVRAM ايضا وهو

Router / Switch # erase start

أسئلة وإجابات المقابلات الشخصية

بعض البروتوكولات الهامة

① SMTP

هو اختصار Simple mail Transfer protocol وهو بروتوكول يستخدم في التعامل مع البريد الالكتروني على شبكة الانترنت وهو البروتوكول المسئول عن عملية ارسال الرسالة وتوجيهها إلى المستقبل المحدد من قبلنا وهو بروتوكول يعمل ويستخدم البورت (25) وهو بروتوكول (TCP) ويعمل على الطبقة السابعة Application layer

② pop

هو اختصار post office protocol وهو بروتوكول يستخدم مع البريد الالكتروني وهو المسئول عن طلب فتح الرسائل أو حذفها أو حفظها وهو المسئول أيضاً عن استلام الرسائل ولكنه ينفذ وظيفته من خلال برنامج وسيط مثل outlook أي أن هذا البروتوكول يسمح للمستخدم بتنزيل جميع رسائل إلى جهازه ومن ثم تزامنها مع إمكانية حذفها من الجهاز الخادم [server] وهو مناسب للمستخدمين ذوي الاتصال الضعيف بالانترنت أو المتقطع أو ذو التكلفة العالية لأنه يمكنهم من تصفح الرسائل في حالة عدم الاتصال بالإنترنت وهذا البروتوكول هو الأكثر استخداماً وله اصدارات مختلفة pop_1 ويستخدم البورت (110) والاصدار الثاني pop_2 ويستخدم البورت (109) والاصدار الحالي pop_3 ويستخدم البورت (110) وهو بروتوكول يعمل في الطبقة السابعة App. layer ويستخدم بروتوكول (TCP)

③ IMAP

هو اختصار Internet message Access protocols وهو البروتوكول المسئول عن الدخول إلى email server وقراءة الرسائل وهو يعمل على الطبقة السابعة App. Layer وهو المسئول عن طلب فتح الرسائل أو حذفها أو حفظها على السيرفر الخاص بالبريد الالكتروني الخاص بك وله أربع اصدارات نستخدم منه الاخير منها وهو يستخدم udp بروتوكول والمنفذ (143)

* ظهرت إصدارات أمنية من البروتوكولات السابقة والتي تؤدي نفس الوظيفة لكن تقوم بعملية تشفير للبيانات لحماية البريد من عمليات القرصنة والتجسس وهي

Secure pop$_3$ (SSLpop) → port 995
IMAp over SSL (IAMps) → port 993
Secure SMtp (ssmtp) → port 465

④ SSL هو اختصار Secure socket layer وهو بروتوكول مسئول عن تشفير البيانات المتنقلة من وإلى متصفح الانترنت والسيرفر ويقوم باستخدام هذه العملية عن طريق مفتاحين [public Key] والآخر [private Key] ويستخدم هذا البروتوكول لتشفير البيانات الحساسة مثل كلمات المرور واسم المستخدم و password أرقام بطاقة الائتمان لذلك يستخدم في مواقع FaCebook و Twitter وغيرها. وهو بروتوكول Tcp ويستخدم البورت 443

س: ما هو الفرق بين HTTp و HTTps ؟

① HTTp هو اختصار Hyper text tranfer protocol وهو البروتوكول الرئيسي المسئول عن نقل البيانات بين المتصفح وسيرفرات الانترنت وهو البروتوكول الأكثر استخداماً لكن البيانات تنقل بطريقة غير مشفرة أي أنه يفتقر للحماية وهو بروتوكول Tcp ويستخدم المنفذ 80

② HTTps هو عبارة عن اختصار Hyper text transfer protocol secure وهو عبارة عن مزيج بين بروتوكول HTTp وبروتوكول SSL ووظيفته هو إنشاء قناة مشفرة وآمنة بين المتصفح وسيرفرات الانترنت أي أنه يوفر الأمان والحماية التي افتقدها HTTp لذلك يستخدم في المواقع مثل Facebook و Twitter وهو بروتوكول Tcp يستخدم البورت 443

س/ ماهو فائدة وجود سبع طبقات في الشبكات ؟

* توحيد معظم مصنعي أجهزة الشبكات تحت منظومة واحدة وقياسية
* تقسيم الاتصال عبر الشبكة إلى أجزاء اصغر وأبسط مما يساهم في عملية تتبع سبب المشاكل وبالتالي حل المشكلة

س/ ماهي ميزات ال UDP عن TCP ؟

*١ UDP أسرع من TCP حيث UDP لا يتمتع بالموثوقية والتعقيد الموجود في TCP وكذلك لا يتطلب اشعار بالاستلام ACK عكس ال TCP
*٢ استهلاك UDP لقدرة المعالج أقل من TCP

س/ ماهو الفرق بين ال DHCP و DNS ؟

DHCP ← مسئول عن توزيع الايبهات للأجهزة بشكل اوتماتيكي
DNS ← مسئول عن ترجمة اسماء المواقع إلى ايبهات ثابتة ومحفوظة على سيرفرات DNS

س/ ما الفرق بين FTP و TFTP ؟

FTP ⟸ هو اختصار File transfer protocol وهو المسئول عن نقل الملفات بين الأجهزة التي تدعم هذه التقنية وهو بروتوكول TCP ويستخدم منفذين المنفذ 20 لنقل البيانات والمنفذ 21 مسئول عن نقل الاوامر Control Connection

TFTP ⟸ نسخة مصغرة من FTP تستخدم تثبيت أنظمة التشغيل وهو اختصار Trivial File Transfer protocol وهو بروتوكول UDP ويستخدم المنفذ 69 وكونه UDP فإنه أسرع من FTP حيث الأخير TCP

س/ لماذا يملك FTP منفذان 20 و 21 ؟

المنفذ 20 هو المسئول عن نقل البيانات بين العميل والسيرفر ويدعى Data Connection بينما المنفذ 21 مسئول عن نقل الاوامر ويدعى Control Connection

س: ما هي خطوات استعادة كلمة السر على روترات سيسكو؟

١* الاتصال من خلال الـ port console

٢* تشغيل الجهاز وأثناء الإقلاع وعند ظهور علامة الهاشتاج ### نضغط على Ctrl + Break للدخول لوضع الـ Rommon

٣* نغير الـ Register file إلى 0x2142 بدلاً من 0x2102

٤-* نعمل Reload للراوتر ونشغل على الإعدادات ونشغل الإعدادات لـ Run عن طريق الأمر # Copy Start Run

٥* نغير كلمة السر الجديدة

٦* نرجع الملف 0x2102 عن طريق الأمر Router(config) #register 0x2102

٧* نحفظ الإعدادات # Copy Run Start

٨* نعمل Reload واستخدم الأمر # Reload

س